2006

Internal Control over Financial Reporting - Guidance for Smaller Public Companies, Volume II : Guidance

Committee of Sponsoring Organizations of the Treadway Commission

COSO

Internal Control over Financial Reporting – Guidance for Smaller Public Companies

Volume II : Guidance

Internal Control over Financial Reporting – Guidance for Smaller Public Companies . Volume II : Guidance

Committee of Sponsoring Organizations of the Treadway Commission

Board Members

Larry E. Rittenberg
COSO Chair

Mark Beasley
American Accounting Association

Nick Cyprus
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

David A. Richards
The Institute of Internal Auditors

Jeffrey Thomson
Institute of Management Accountants

PricewaterhouseCoopers LLP – Author

Principal Contributors

Miles Everson (Project Leader)
Partner
New York City

Frank Martens
Director
Vancouver, Canada

Frank Frabizzio
Partner
Philadelphia

Tom Hyland
Partner
New York City

Paul Tarwater
Partner
Dallas

Mark Cohen
Senior Manager
Boston

Erinn Hansen
Senior Manager
Philadelphia

Mario Patone
Manager
Philadelphia

Chris Paul
Senior Associate
Boston

Shurjo Sen
Manager
New York City

Project Task Force to COSO

Guidance

Deborah Lambert (Chair)
Partner
Johnson, Lambert & Co.

Christine Bellino
Jefferson Wells International, Inc.

Joseph V. Carcello
Professor of Accounting
University of Tennessee

Rudolph J. J. McCue
WHPH, Inc.

Douglas F. Prawitt
Professor of Accounting
Brigham Young University

Malcolm Schwartz
CRS Associates LLC

Members at Large

Carolyn V. Aver
CFO
Agile Software Corporation

Kristine M. Brands
Director of Financial Systems
Inamed, A Division of Allergan

Serena Dávila
Director for Private Companies & Small Business
Financial Executives International

Gus Hernandez
Partner
Deloitte & Touche, LLP

Brian O'Malley
Chief Audit Executive
Nasdaq

Andrew Pinnero
JLC/Veris Consulting LLC

Pamela S. Prior
Director of Internal Control & Analysis
Tasty Baking Company

James K. Smith, III
Vice President & CFO
Phonon Corp.

Dan Swanson
President and CEO
Dan Swanson & Associates

Dominique Vincenti
Director of Professional Practice
The Institute of Internal Auditors

Kenneth W. Witt
American Institute of Certified Public Accountants

Observer

Jennifer Burns
Professional Accounting Fellow
Securities and Exchange Commission

Internal Control over Financial Reporting – Guidance for Smaller Public Companies

Volume II : Guidance

June 2006

1 2 3 4 5 6 7 8 9 0 MC&D 0 9 8 7 6

Foreword

COSO is pleased to present this guidance to assist smaller public companies in implementing the 1992 COSO *Internal Control—Integrated Framework*. We believe the guidance will be helpful to smaller businesses as they explore cost-benefit approaches to achieve their financial reporting objectives. This guidance contains numerous examples that have been effectively used by smaller business to address its internal control objectives.

The COSO task force has considered the comment letters received during the exposure period of the preliminary guidance. A number of positive changes have been made in response to the comment letters we received, including:

- An enhanced focus on achieving the objectives of internal control
- An enhanced view of internal control as a process
- An articulation of fundamental principles that underlie each of the internal control components and a clearer linkage to controls a company might implement
- A recognition that management must make cost-effective decisions in determining which controls to implement.

The COSO framework is robust, but it depends on the ability of management and other parties to implement objectives-based and principles-based approaches to internal control. We continue to believe that businesses are enhanced by having the flexibility of choosing the most appropriate controls for them to achieve their internal control objectives. While the guidance is oriented towards smaller businesses, we believe it will be useful for every organization, public or private, large or small, in implementing effective internal control over financial reporting.

In developing this guidance, the COSO board selected a project team from PricewaterhouseCoopers led by Miles Everson and Frank Martens. We also utilized a large task force of individuals who were experienced with smaller businesses. They devoted countless hours thinking about the basic concepts of internal control, reading drafts of the guidance, and contributing control approaches and examples. This project was clearly a team effort. All of the individuals listed on the inside cover pages were significant contributors to the guidance. However, I would like to recognize a few for their leadership and contributions. They are Christine Bellino of Jefferson-Wells, Joe Carcello of the University of Tennessee, Doug Prawitt of Brigham Young University, and Malcolm Schwartz of CRS Associates, all of whom led task forces dealing with the principles underlying the internal control framework. In addition, I want to thank Jennifer Burns, a practice fellow at the SEC for her significant contributions to our thought processes as we developed the guidance.

The COSO board was actively involved throughout the development of this guidance. We welcome your feedback and remain committed to improving the quality of financial reporting, risk management, and control.

Larry E. Rittenberg
Chair, COSO

June 2006

Internal Control over Financial Reporting – Guidance for Smaller Public Companies

Volume II : Guidance

June 2006

Contents

Overview 1

I. Control Environment 19
- Principle 1 Integrity and Ethical Values 20
- Principle 2 Board of Directors 23
- Principle 3 Management's Philosophy and Operating Style 29
- Principle 4 Organizational Structure 31
- Principle 5 Financial Reporting Competencies 33
- Principle 6 Authority and Responsibility 35
- Principle 7 Human Resources 38

II. Risk Assessment 43
- Principle 8 Financial Reporting Objectives 44
- Principle 9 Financial Reporting Risks 47
- Principle 10 Fraud Risk 52

III. Control Activities 55
- Principle 11 Integration with Risk Assessment 56
- Principle 12 Selection and Development of Control Activities 58
- Principle 13 Policies and Procedures 62
- Principle 14 Information Technology 66

IV. Information and Communication 75
- Principle 15 Financial Reporting Information 76
- Principle 16 Internal Control Information 78
- Principle 17 Internal Communication 81
- Principle 18 External Communication 84

V. Monitoring 87
- Principle 19 Ongoing and Separate Evaluations 88
- Principle 20 Reporting Deficiencies 92

Appendices 95
- A. Methodology 97
- B. Consideration of Comment Letters 99
- C. Glossary of Selected Terms 103
- D. Acknowledgments 105

Overview

This document provides guidance for smaller public companies in using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control – Integrated Framework* as it relates to the effectiveness of internal control over financial reporting. Internal control over financial reporting is defined in the *Framework* as a process, effected by a company's board of directors, management and other personnel, designed to provide reasonable assurance regarding the reliability of published financial statements. This document describes ways to accomplish that objective in a cost-effective manner.

Many changes have taken place in financial reporting and the related legal and regulatory environment since the *Framework* was issued. Significantly, the Sarbanes-Oxley Act was passed by the United States Congress and signed into law by the President in 2002. Section 404 of the Act requires management annually to assess and report on the effectiveness of a public company's internal control over financial reporting. Due to unique challenges faced by smaller companies in implementing Section 404, and in using the *Framework* in connection with that effort, the Securities and Exchange Commission's Chief Accountant requested that COSO develop this guidance.

This document neither replaces nor modifies the *Framework*, but rather provides guidance on how to apply it in designing and implementing cost effective internal control over financial reporting. Although not its primary purpose, this guidance also may be useful to management in more efficiently assessing internal control effectiveness, in the context of assessment guidance provided by regulators.

The guidance herein is consistent with the *Framework's* definitions, components, and criteria for effective internal control. Because the *Framework* is applicable to all companies, and its content – including some direction on how the *Framework* may be applied in a smaller business environment – is not repeated here, it is suggested that readers refer to the *Framework* in conjunction with using this guidance.

While this guidance is directed to management of smaller public companies, it may also be useful to management of larger public businesses, private companies, and other organizations. Similarly, this guidance is not directed to external audit firms, but they may wish to consider it to gain a better understanding of how the *Framework* can be applied cost effectively by their smaller public company clients.

This report is in three volumes. The first is an *Executive Summary*, providing a high level summary for companies' boards of directors and senior management.

This second volume provides an overview of internal control over financial reporting in smaller businesses, including descriptions of company characteristics and how they affect internal control, challenges smaller businesses face, and how management can use the *Framework*. Presented are twenty fundamental principles drawn from the *Framework*, together with related attributes, approaches and examples of how smaller businesses can apply the principles in a cost-effective manner.

The third contains illustrative tools to assist management in evaluating internal control. Managers may use the illustrative tools in determining whether the company has effectively applied the principles.

It is expected that senior management will find the *Executive Summary* and *Overview* chapter of this Volume II of particular interest and might refer to certain of the following chapters as needed, and that other managers will use Volumes II and III as a reference source for guidance in those areas of particular need.

Costs and Benefits of Internal Control

Management and other stakeholders of public companies, particularly smaller ones, have focused great attention on the cost of complying with Sarbanes-Oxley Act Section 404. Significant attention has been given to the cost of maintaining effective internal control systems, as well as costs associated with assessing the system and remediating weaknesses in preparation for reporting publicly thereon.

Attention also has been given to the benefit side of the cost-benefit equation. Among the most significant benefits of effective internal control is the ability of companies to access the capital markets, providing capital driving innovation and economic growth. Such access of course comes with responsibilities to effect timely and accurate financial reporting to stakeholders, including shareholders, creditors, capital providers, regulators and parties with which a company has direct contractual relationships. Effective internal control over financial reporting supports reliable financial reporting, which in turn enhances investor confidence in providing the requisite capital.

Other benefits of effective internal control over financial reporting include:

- Reliable and timely information supporting management's decision-making on such matters as product pricing, capital investment, and resource deployment.
- Consistent mechanisms for processing transactions across an organization enhancing speed at which transactions are initiated and settled, reliability of related recordkeeping, and ongoing integrity of data.
- Ability and confidence to accurately communicate business performance with business partners and customers.

While the incremental cost to evaluate and report on internal control has become a primary focal point for many corporate stakeholders, it is useful to balance costs with the related benefits.

Additionally, users of this guidance should be mindful that because internal controls are interrelated, controls established primarily for financial reporting purposes also can support a company's operations and compliance objectives. The converse holds as well, such that it is useful to consider the financial reporting implications of controls directed primarily at operations and compliance objectives.

Large versus Smaller Companies

Internal control systems are developed in all companies to support ongoing company activities, facilitate growth, and otherwise carry out responsibilities towards achieving business objectives. Internal control involves identifying and managing risks to financial reporting that are inherent in all businesses. Such basic concepts as integrity and ethical values, reconciliations, and management review are important to all organizations. Indeed, there are fewer differences than many perceive in how internal control is established in smaller companies versus their larger counterparts.

Although the basic principles of internal control in smaller companies mirror those of larger ones, implementation approaches vary. For example, all public companies have boards of directors with oversight responsibilities related to financial reporting. A smaller company, however, may have a less complex business structure and operations and more frequent communication with directors, enabling different approaches to board oversight. Similarly, while all public companies are required to have a whistle-blower program, differences in relative volume of reported events may require reporting to an identified internal staff function in a large company, but allow direct reporting to a smaller company's audit committee chair.

Smaller companies typically have unique advantages over larger ones that can contribute to effective internal control. These may include wider spans of control by senior managers and greater direct interaction with company personnel. For instance, smaller companies may find informal staff meetings highly effective for communicating information relevant to financial reporting, whereas larger companies may need more formal mechanisms such as written reports, intranet portals, or periodic formal meetings or conference calls to communicate similar matters.

Smaller companies compete by identifying innovative and cost-effective mechanisms within the marketplace. While their management cannot reject the need for effective internal control simply on the grounds that the company is small, they can utilize similar innovative thinking to accomplish their financial reporting objectives in a cost-effective manner.

Characteristics of "Smaller" Companies

Clearly, many different perceptions exist as to what constitutes a "small" business. Some think of a local, family-owned hardware store or corner bakery as typical small businesses. Others consider small business as a start-up services company that generates several million dollars in annual sales. Still others see a small company as one that has been public for many years manufacturing an innovative product which now generates annual revenue of several hundred million dollars, with hopes that future growth will catapult it to the Fortune 500. Depending on perspective, any or all of these companies may be considered "small."

While there is a tendency to want a "bright line" to define business size as small, medium-size or large, this guidance does not provide such definitions in terms of revenue, capitalization, or otherwise. That is the role of regulators or other parties.

This document uses the term "smaller" rather than "small" business, suggesting there is a wide range of companies to which this guidance is directed. The focus here is on businesses – referred to here as "smaller" – that have many of the following characteristics:

- Fewer lines of business, and fewer products within lines
- Concentration of marketing focus, by channel or geography
- Leadership by management with significant ownership interest or rights
- Fewer levels of management, with wider spans of control
- Less complex transaction processing systems
- Fewer personnel, many having a wider range of duties
- Limited ability to maintain deep resources in line as well as support staff positions such as legal, human resources, accounting and internal auditing.

The last bulleted item above reflects a frequent reality causing smaller businesses to be lower on the economies-of-scale curve. This often is the case with regard to per-unit cost to produce product or provide service, but not always. Indeed, many smaller businesses achieve competitive advantage in cost savings through innovation, lower overhead – retaining fewer people and substituting variable for fixed costs via a part-time workforce or variable compensation plans – and a narrower focus in terms of product, location, and complexity.

Economies of scale often is a factor with respect to support functions, including those directly relevant to internal control over financial reporting. For example, establishing an internal audit function within a hundred-million-dollar company likely would require a larger percentage of the company's economic resources than would be the case for a multi-billion dollar entity. Certainly, the smaller company's internal audit function would be smaller, and might rely on co-sourcing or outsourcing in order to provide needed skills, where the larger company's function might be significantly larger with a broad range of experienced personnel in house. But in all likelihood the relative cost for the smaller company would be higher than for the larger one.

None of the above characteristics by themselves are definitive. Certainly, size by whatever measure – revenue, personnel, assets, or other – affects and is affected by these characteristics, and shapes our thinking about what constitutes "smaller."

Meeting Challenges in Attaining Cost-Effective Internal Control

The characteristics of smaller companies tend to provide significant challenges for cost-effective internal control. This particularly is the case where managers view control as an administrative burden to be added onto existing business systems, rather than recognizing the business need for and benefit of effective internal control that is integrated with core processes.

Among the challenges are:

- Obtaining sufficient resources to achieve adequate segregation of duties
- Management's ability to dominate activities, with significant opportunities for improper management override of processes in order to appear that business performance goals have been met
- Recruiting individuals with requisite financial reporting and other expertise to serve effectively on the board of directors and audit committee
- Recruiting and retaining personnel with sufficient experience and skill in accounting and financial reporting
- Taking critical management attention from running the business in order provide sufficient focus on accounting and financial reporting
- Controlling information technology and maintaining appropriate general and application controls over computer information systems with limited technical resources.

Despite resource constraints, smaller businesses usually can meet these challenges and succeed in attaining effective internal control in a reasonably cost-effective manner – accomplished in a variety of ways, discussed in the following paragraphs.

Segregation of Duties

Appropriate segregation of duties is achieved when one or more employees or functions acts as a check and balance on the activities of another, such that no one individual has control over conflicting phases of a transaction or activity.

Assigning different people responsibility for authorizing transactions, recording transactions, reconciling information, and maintaining custody of assets reduces opportunity for any one employee to conceal errors or perpetrate fraud in the normal course of his or her duties. For example, if one person executes a sale, that person should not record the transaction, handle the cash receipt, have authority for or access to cash receipts records, and reconcile the bank account.

Due to resource constraints, many smaller companies have limited numbers of employees performing these types of functions, sometimes resulting in inadequate segregation of duties. There are, however, actions management can take to compensate for this circumstance. Following are some types of controls that can be implemented:

- *Review reports of detail transactions* – Managers review on a regular and timely basis system reports of the detailed transactions.
- *Review selected transactions* – Managers select transactions for review of supporting documents.
- *Take periodic asset counts* – Managers periodically conduct counts of physical inventory, equipment or other assets and compare them with the accounting records.
- *Check reconciliations* – Managers from time to time review reconciliations of account balances such as cash or perform them independently.

Segregation of duties is not an end in itself, but rather a means of mitigating a risk inherent in processing. When developing or assessing controls that address risks to reliable financial reporting in a company with limited ability to segregate duties, management should consider whether other controls satisfactorily address these risks and are applied conscientiously enough to reduce risk to an acceptable level.

Management Override

Many smaller businesses are dominated by the company's founder or other strong leader who exercises a great deal of discretion and provides personal direction to other personnel. This positioning may be key to enabling the company to meet its growth and other objectives, and can also contribute significantly to effective internal control over financial reporting. With this leader's in-depth knowledge of different facets of the business – its operations, processes, array of contractual commitments and business risks – he or she is positioned to know what to expect in reports generated by the financial reporting system and to follow up as needed where unanticipated variances surface. Such concentration of knowledge and authority, however, comes with a downside – the company leader typically is able to override established procedures for reliable financial reporting.

There are a few basic but important things that can help to mitigate the risk of management override.

- One is maintaining a corporate culture where integrity and ethical values are held in high esteem, embedded throughout the organization and practiced on an every day basis. This can be supported and reinforced by recruiting, compensating and promoting individuals where these values are appropriately reflected in behavior.

- Another is an effective whistle-blower program, where company personnel feel comfortable reporting any improprieties, regardless of the level at which they may be committed. Importantly, there must be ability to maintain anonymity and confidence that reported matters will be investigated thoroughly and acted upon, appropriately without reprisals. It usually is important that where circumstances warrant matters can be reported directly to the board or audit committee.
- Where available, an effective internal audit function is positioned to detect instances of wrongdoing, even at the highest company levels. Ready access to relevant information and ability to communicate directly with the board or audit committee are key factors.
- And, a qualified board of directors and audit committee that takes its responsibilities seriously performs a critical role in preventing or detecting instances of management override.

Such practices mitigate the risk of impropriety and promote accountability of company leadership, while gaining the unique advantages of cost-effective internal control in a smaller public company environment.

Board of Directors

The preceding paragraphs highlight the need for a board of directors, usually with financial reporting oversight responsibilities conducted via its audit committee, with requisite qualities that perform their oversight responsibilities well. An effective board will have a critical mass of independent directors, financial reporting expertise, timely and relevant information and sufficient resources and time to understand and deal with the issues, and directors' commitment to carry out their responsibilities with due care and keep the company's and its shareholders' interests in the fore.

Effective boards and audit committees objectively review management's judgments and help identify and diagnose unusual activity potentially impacting financial reporting. With appropriate knowledge, attention, and communication, they are positioned to utilize the recommendations of internal and external auditors in evaluating the overall quality of the company's controls and financial reports. As such, these boards and audit committees can provide an effective means of offsetting the effects of improper management override. This is especially the case with smaller company boards, where directors typically have an in-depth knowledge of what usually are relatively straightforward business operations and communicate more closely with a broader range of company personnel.

Many smaller businesses, however, face challenges attracting independent directors with the desired skills and experience. Whether due to inadequate knowledge of the company and its people, the company's limited ability to provide compensation commensurate with board responsibilities, a sense that the chief executive might be unaccustomed or unwilling to appropriately share governance responsibilities, or concerns about potential personal liability, smaller companies have traditionally faced challenges in attracting directors. Recently, however, especially with new stock exchange listing standards and related calls for improved corporate governance, smaller companies have looked to bring more independent directors with appropriate qualifications onto the board. Some companies have been willing to address the concerns of desired board candidates and have expanded their search to broader populations with financial and accounting and other valued expertise, shaping the kind of board that not only provides appropriate monitoring of senior management, but also provides value-added advice and counsel.

Qualified Accounting Personnel

For effective internal control, a company needs sufficient accounting and financial reporting expertise to ensure development of reliable financial statements. Some smaller companies, however, are challenged in obtaining qualified accounting personnel, especially at more senior levels where a high level understanding of accounting principles and financial reporting standards and application is required.

There are several approaches to deal with this circumstance. One is to devote additional corporate resources to bring qualified individuals on board. Another is to avoid unnecessary complexity in corporate structure or nature of business transactions. This is not to suggest avoiding opportunities for profitable growth, but rather to avoid complexity requiring greater sophistication and breadth of accounting knowledge where simplicity accomplishes the same business objectives. Some smaller companies have invested in development of their most senior financial officer, providing education and training enabling that individual to adequately carry out the associated responsibilities.

In that regard, there has been some uncertainty in the extent to which a chief financial officer or other accounting personnel are permitted to discuss technical accounting and reporting issues with outside parties, particularly the company's external auditor. Regulators have provided guidance indicating that specified types of communications with the external auditor are viewed as normal business practice, and do not drive a conclusion that the company's personnel are lacking in the requisite ability to make their own decisions in developing the needed financial reports.

Management's Focus on Accounting and Financial Reporting

Management of smaller companies typically concentrate their attention on strategic and day-to-day issues in running and working to profitably grow the business. Senior managers frequently are concerned about devoting additional amounts of their time to accounting and reporting matters at the "expense" of the "real" business.

In this regard it is useful to recognize that procedures already being performed for operational business purposes are likely also to contribute to effective internal control over financial reporting. Taking just one example, a company's sales vice president keeps abreast of sales by product and region via daily "flash" reports from district heads. This is done primarily for operational purposes, to be positioned to react to unanticipated sales performance. But because the sales vice president also relates that information to sales reported by the accounting system and points out discrepancies to the accounting department, this procedure also serves as a valuable financial reporting control.

Reality is that in the current environment senior management need to devote additional time to financial reporting matters. But where existing practices are leveraged in accomplishing financial reporting objectives, the incremental time can be limited.

Information Technology

Another reality is that many smaller companies do not have the extensive technical resources necessary to develop, maintain and operate software in an adequately controlled manner. Thus, these companies consider alternatives to meet their information and control needs.

Many smaller companies use software developed and maintained by others. These packages still require controlled implementation and operation, but many of the risks associated with in-house developed systems are reduced. For example, typically there is less need for program change controls, inasmuch as changes are done exclusively by the developer company, and generally

smaller company's personnel don't have the technical expertise to attempt to make unauthorized program modifications.

Commercially developed packages can bring additional advantages. Such packages may provide embedded facility for controlling which employees in the company can access or modify specified data, performing checks on data processing completeness and accuracy, and maintaining related documentation.

Automated Controls

Many accounting software packages come with a variety of built-in application controls, which can improve consistency of operation and processing results, automate reconciliations, facilitate reporting of exceptions for management review, and support proper segregation of duties. Many larger businesses take advantage of these capabilities, ensuring "flags" or "switches" are properly set to take advantage of the software's capabilities.

Smaller businesses may want to make the investment, engaging external implementation support where necessary, in order to add efficiencies in achieving the company's objectives. Once properly implemented, reports can be generated on changes or exceptions to processing, ensuring segregation of duties and promoting both effectiveness and efficiency in the internal control system.

There is another area related to computer application controls where smaller companies can achieve efficiencies gained by many of their larger counterparts – having to do with attention given to ensuring that application controls continue to operate effectively. Many companies in their first year of reporting publicly on internal control over financial reporting expended significant time and effort testing controls imbedded in computer application programs to determine whether they were operating as planned. There now is greater recognition that once application controls have been determined to be effective, there normally is little need to directly test such controls in subsequent periods. This is because where a company determines each year that its IT general controls are effective, management has comfort that the application controls have not changed, or if they have, the revised controls have been appropriately designed, tested, and implemented during the change process, and continue to operate effectively.

Under this scenario manual user controls reacting to exception reports and other outputs of application controls still need attention, as may also be the case with respect to certain application controls of an extremely critical nature where alternative means of determining propriety of processing results are not available. And management might decide to verify application control effectiveness on a cycle basis over time. For the most part, however, strong general controls deemed to be effective over time provide significant efficiencies with regard to attention needed to the continued and proper application of computer application controls.

Monitoring Activities

The monitoring component is an important part of the *Framework*, where a wide range of activities routinely performed by managers in running a business can provide information on the functioning of other components of the internal control system. Management of many smaller businesses regularly perform such procedures, but have not always taken sufficient "credit" for their contribution to internal control effectiveness. These activities, usually performed manually and sometimes supported by computer software, should be fully considered in designing or assessing internal control.

In addition to the relevance of ongoing monitoring activities to effective internal control sometimes not being well understood, there frequently is confusion between whether a certain procedure is a control activity or a monitoring control, because there can be a fine line between the two. Indeed, there is overlap between the components, and in some cases the same control arguably could fall within either one.

A determination of whether a particular control is a control activity or a monitoring control can depend on whether its primary purpose is to perform an initial check on processing of accounting information, or whether it provides comfort on whether controls serving as that initial check continue to operate effectively over time. The former would normally be viewed primarily as a control activity, the latter a monitoring control.

An example relates to certain computer software, which has long been utilized in large companies and is becoming increasingly available to smaller businesses. New software has come onto the market that automates determining when errors or improprieties in processing may have occurred or segregation of duties compromised. Depending on the precise nature of these controls, or perhaps perspective, the controls might be deemed to be general computer controls – a part of the control activities component – or they might be viewed as tracking the effectiveness of the general computer controls, falling under the monitoring component.

The component into which a procedure falls, however, is not as important as recognizing whether and how the procedure contributes to effective and efficient internal control. While terminology is important in communicating about control issues, more relevant here is that, regardless into which component a particular control is deemed to fall, the controls described above can be an important contributor to internal control efficiency.

From a different perspective, there is another way monitoring activities can promote efficiency, in connection with assessing internal control effectiveness. Consider a company where in the first year of reporting publicly on internal control management performed all necessary assessment procedures, including documenting controls and determining adequacy of design, testing operating effectiveness of controls, and remediating deficiencies. The company addressed all five components, determined there were no material weaknesses and concluded that the system was effective, and the company's external auditor concurred in the assessment. In the second year, management could begin the process again, updating the documentation and repeating all the other elements of the prior year's assessment. Indeed, this is the approach taken by a number of companies.

A different approach can be taken, however, to promote efficiency. This involves focusing on monitoring procedures already in place, or that might be added with little additional effort, in order to identify significant changes since the prior year. Particular focus in monitoring can be given to changes in computerized accounting processes, but with attention also given to any changes in the control environment, control activities conducted at higher levels, and the like. By focusing on these changes, management can gain important information on where to target more detailed testing of the control system.

Of course, for effective internal control, all five components must be appropriately designed and operating effectively, and some testing of each component is necessary for each public report to be issued. But with highly effective monitoring activities, there can be tradeoffs in components and in scope and targeting of assessment work, resulting in greater efficiency overall.

Indeed, some companies have looked to convert what has been a time-consuming annual project into more of an ongoing process, making the effort more self-sustaining and efficient. Ongoing monitoring procedures, including recently available and improved software, supplemented by separate evaluative procedures, can be useful in efficiently achieving those objectives.

Achieving Further Efficiencies

In addition to considering the above, companies can gain additional efficiencies in designing and implementing or assessing internal control by focusing on only those financial reporting objectives directly applicable to the company's activities and circumstances, taking a risk based approach to internal control, right sizing documentation, viewing internal control as an integrated process, and considering the totality of internal control.

Focusing on Financial Reporting Objectives

The COSO framework recognizes that an entity must first have in place an appropriate set of financial reporting objectives. At a high level, the objective of financial reporting is to prepare reliable financial statements, which involves attaining reasonable assurance that the financial statements are free from material misstatement. Flowing from this high level objective, management establishes supporting objectives related to the company's business activities and circumstances and their proper reflection in the company's financial statement accounts and related disclosures. These objectives may be influenced by regulatory requirements or by other factors that management may choose to incorporate when setting its objectives.

Efficiencies are gained by focusing only those objectives directly applicable to the business and related to its activities and circumstances that are material to the financial statements. Experience shows that this can be most efficiently accomplished by beginning with a company's financial statements and identifying supporting objectives for those business activities, processes and events that can materially affect the financial statements. In this way, a basis is formed for giving attention only to what is truly relevant to the reliability of financial reporting for that company.

Focusing on Risk

While management considers risks in several respects, its overarching consideration is the risks to key objectives, including the risks to reliable financial reporting. Risk-based means focusing on quantitative and qualitative factors that potentially affect the reliability of financial reporting, and identifying where in transaction processing or other activities related to financial statement preparation something could go wrong. By focusing on key objectives management can tailor the scope and depth of risk assessments needed. Often risk is considered in the context of initially designing and implementing internal control, where risks to objectives are identified and analyzed to form a basis for determining how the risks should be managed. Another is in the context of assessing whether internal control is effective in mitigating risks to objectives.

In the context of assessing internal control effectiveness, there sometimes is a tendency to consider internal control using generic lists of controls appropriate to a "typical" organization. While these tools in questionnaire or other form may be useful, an unintended result is that management sometimes focuses on "standard" or "typical" controls that simply are not relevant to the company's financial reporting objectives or risks associated with those objectives. A related problem encountered is

starting assessments with the details of accounting systems and documenting them in extreme depth without recognizing whether the entirety of processes are truly relevant to achieving reliable financial reporting. This is not to say that such approaches cannot be useful, as they can be. However, whatever approach is followed, efficiencies are gained when attention is directed to the objectives management has established specific to the company's business activities and circumstances. A targeted approach helps to ensure attention is given only to those risks that are directly relevant to the company.

Viewing Internal Control as an Integrated Process

It is useful to view the *Framework's* five internal control components as comprising an integrated process, which indeed internal control is. A process perspective highlights the interrelationship of the components, and recognizes that management has flexibility in choosing controls to achieve its objectives and that an organization can adjust and improve its internal control over time.

As noted, the internal control process begins with management setting financial reporting objectives relevant to the company's particular business activities and circumstances. Once set, management identifies and assesses a variety of risks to those objectives, determines which risks could result in a material misstatement in financial reporting, and determines how the risks should be managed through a range of control activities. Management implements approaches to capture, process and communicate information needed for financial reporting and other components of the internal control system. All this is done in context of the company's control environment, which is shaped and refined as necessary to provide the appropriate tone at the top of the organization and related attributes. These components all are monitored to help ensure that controls continue to operate properly over time. An overview of *Framework's* components working together from a process perspective can be depicted as follows:

An assessment of internal control considers whether the components, all logically interrelated, are working together to accomplish the company's financial reporting objectives.

Right-sizing Documentation

Documentation of business processes and procedures and other elements of internal control systems is developed and maintained by companies for a number of reasons. One is to promote consistency in adhering to desired practices in running the business. Effective documentation assists in communicating what is to be done, and how, and creates expectations of performance. Another purpose of documentation is to assist in training new personnel and as a refresher or reference tool for other employees. Documentation also provides evidence to support reporting on internal control effectiveness.

The level and nature of documentation varies widely by company. Certainly, large companies usually have more operations to document, or greater complexity in financial reporting processes, and therefore find it necessary to have more extensive documentation than smaller ones. Smaller companies often find less need for formal documentation, such as in-depth policy manuals, systems flowcharts of processes, organization charts, job descriptions, and the like. In smaller companies, typically there are fewer people and levels of management, closer working relationships and more frequent interaction, all of which promotes communication of what is expected and what is being done. A smaller business, for example, might document human resources, procurement or customer credit policies with memoranda and supplement the memoranda with guidance provided by management in meetings. A larger company will more likely have more detailed policies (or policy manuals) to guide their people in better implementing controls.

Questions arise as to the extent of documentation needed to deem internal control over financial reporting as effective. The answer is, of course, it depends on circumstances and needs. Some level of documentation is always necessary to assure management that its control processes are working, such as documentation to help assure management that all shipments are billed, or periodic reconciliations are performed. In a smaller business, however, management is often directly involved in performing control procedures and for those procedures there may be only minimal documentation because management can determine that controls are functioning effectively through direct observation. However, there must be information available to management that the accounting systems and related procedures, including actions taken in connection with preparation of reliable financial statements, are well designed, well understood, and carried out properly.

When management asserts to regulators, shareholders or other third parties on the design and operating effectiveness of internal control over financial reporting, management accepts a higher level of personal risk and typically will require documentation of major processes within the accounting systems and important control activities to support its assertions. Accordingly, management will review to determine whether its documentation is appropriate to support its assertion. In considering the amount of documentation needed, the nature and extent of the documentation may be influenced by the company's regulatory requirements. This does not necessarily mean that documentation will or should be more formal, but it does mean that there needs to be evidence that the controls are designed and working properly.

In addition, when an external auditor will be attesting to the effectiveness of internal control, management will likely be expected to provide the auditor with support for its assertion. That support would include evidence that the controls are properly designed and are working effectively. In considering the nature and extent of documentation needed by the company, management should also consider that the documentation to support the assertion that controls are working properly will likely be used by the external auditor as part of his or her audit evidence.

There may still be instances where policies and procedures are informal and undocumented. This may be appropriate where management is able to obtain evidence captured through the normal conduct of the business that indicates personnel regularly performed those controls. However, it is important to keep in mind that control processes, such as risk assessment cannot be performed entirely in the mind of the CEO or CFO without some documentation of the thought process and management's analysis. Many of the examples contained later in this guidance illustrate how management can capture evidence through the normal course of business.

Documentation of internal control should meet business needs and be commensurate with circumstances. The extent of documentation supporting design and operating effectiveness of the five internal control components is a matter of judgment, and should be done with cost-effectiveness in mind. Where practical, the creation and retention of evidence should be embedded with the various financial reporting processes.

Considering the Totality of Internal Control

All five components of internal control set forth in the *Framework* (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring) are important to achieving the objective of reliable financial reporting. Determining whether a company's internal control system is effective involves a judgment resulting from an assessment of whether the five components are present and functioning effectively without material weakness.

Each of the *Framework's* five components should not be viewed as an "end in itself." Rather the components should be viewed as an integrated system working together to reduce risk to reliable financial reporting to an acceptable level. Importantly, although all five criteria must be satisfied, this does not mean that each component should function identically, or even at the same level, in every company. Some trade-offs may exist between components. Because controls can serve a variety of purposes, controls in one component can serve the purpose of controls that might normally be present in that or another component. Additionally, controls can differ in the degree to which they address a particular risk, so that several controls, each with limited effect, together can be satisfactory. Thus, management considers the contribution made by each internal control component in sufficiently reducing this risk.

From a risk perspective, each of the components serves a purpose, working together to mitigate risks to reliable financial reporting. Looking for example at the control environment, a commitment to financial expertise reduces risk of accounting errors due to judgment, and effective oversight activities by the board and audit committee reduces risk related to management override. With respect to the monitoring component, management's review of weekly reports and investigation of unexpected results can mitigate risks related to errors in processing accounting transactions. Importantly, the components are related and mutually supportive in reducing risk to an acceptable level.

Examples provided here illustrate how the totality of internal control may be viewed, with the first example describing how elements of different components work together to achieve an objective, and both examples showing how a strong control in one component can reduce the need for related controls in another.

A manufacturing company's management considers risks related to the existence, completeness and valuation of certain transactions/accounts, focusing on potential misstatements caused by processing errors, errors due to misjudgments, and the potential of improprieties through

management override. Controls directed at these risks include those in the company's control environment, which provides a commitment to financial expertise in its chief financial officer and others in the accounting function, maintenance of a management philosophy to generally avoid complexity in business structure and transactions, and effective oversight activities by the audit committee. The company's risk assessment activities identify where in the processing stream errors or fraud might occur. Information systems are designed to properly record and account for the transactions, and control activities include appropriate checks for completeness and accuracy of processing, except that certain duties are carried out by one individual with conflicting responsibilities.

In this example, management decides that although controls in the control activities component related to segregation of duties are lacking in certain respects, additional controls in the monitoring can help to reduce risk to reliable financial reporting to an acceptably low lever. These include the CFO's detailed review of reports related to processing by the individual with conflicting responsibilities and operating managers' review of weekly reports and follow up on unexpected results. Taken as a whole, the system provides reasonable assurance that these transaction types are appropriately accounted for.

A mining company with foreign operations does not have adequate general computer controls over production system processing at a foreign location, resulting in risk related to occurrence of activity and completeness of processing of production costs. To mitigate the risk, management implemented corporate office control activities that include reconciliation of reported extractions with on-sight supervisors' production reports, equipment usage and time records, as well as comparison to historical norms, with any differences promptly investigated. In this case, sufficient comfort is gained on the reliability of financial reporting of mining production with these controls in place.

Many companies' assessments of internal control effectiveness have involved a primary focus on the control activities component. As illustrated by these examples, although control activities and each of the other components must be present and functioning effectively, that doesn't mean that every element of control activities relative to every type of transaction processing must be functioning effectively.

In another example, a community bank credit analyst has responsibility for performing specified credit checks on new loan applications before passing the documentation to the branch manager for review and approval. In this case, the branch manager recognizes that the analysts' procedures are not always performed thoroughly. The manager expanded the scope and depth of her review procedures, which coupled with her direct knowledge of the vast majority of the applicants was sufficient to support a conclusion that the credits met the bank's standards.

Effective internal control does not necessarily mean that the "gold standard" of control is built into every process. These examples illustrate how there can be identified classes of transactions for which a control weakness in one component can be mitigated by other controls in that component or in another component that are strong enough such that the totality of control is sufficient to reduce the risk of misstatement to an acceptable level.

Applying Principles in Achieving Effective Internal Control over Financial Reporting

This guidance provides a set of twenty basic principles representing the fundamental concepts associated with and drawn directly from the five components of the internal control *Framework*. The principles, along with the references to more detailed information in this volume, are as follows:

Controls Environment		Page
1.	**Integrity and Ethical Values** – Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.	20
2.	**Board of Directors** – The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.	23
3.	**Management's Philosophy and Operating Style** – Management's philosophy and operating style support achieving effective internal control over financial reporting.	29
4.	**Organizational Structure** – The company's organizational structure supports effective internal control over financial reporting.	31
5.	**Financial Reporting Competencies** – The company retains individuals competent in financial reporting and related oversight roles.	33
6.	**Authority and Responsibility** – Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.	35
7.	**Human Resources** – Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.	38
Risk Assessment		
8.	**Financial Reporting Objectives** – Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting .	44
9.	**Financial Reporting Risks** – The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.	47
10.	**Fraud Risk** – The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.	52
Control Activities		
11.	**Integration with Risk Assessment** – Actions are taken to address risks to the achievement of financial reporting objectives.	56
12.	**Selection and Development of Control Activities** – Control activities are selected and developed considering their cost and potential effectiveness in mitigating risks to the achievement of financial reporting objectives.	58
13.	**Policies and Procedures** – Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.	62
14.	**Information Technology** – Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.	66

(continued next page)

Information and Communication	Page
15. **Financial Reporting Information** – Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.	76
16. **Internal Control Information** – Information needed to facilitate the functioning of other control components is identified, captured, used, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.	78
17. **Internal Communication** – Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.	81
18. **External Communication** – Matters affecting the achievement of financial reporting objectives are communicated with outside parties.	84
Monitoring	
19. **Ongoing and Separate Evaluations** – Ongoing and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time.	88
20. **Reporting Deficiencies** – Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.	92

Attributes

Supporting each principle are attributes, representing characteristics associated with the principle. Although each attribute generally is expected to be present within a company, it may be possible to apply a principle without every listed attribute being present.

Approaches

Approaches describe how smaller companies can apply a principle. Many of the approaches included here are being used by managers of smaller businesses. Each approach is referenced to related attributes, which may be useful in considering which approaches to use in achieving the principle.

Further, there is no expectation of a one-to-one relationship between a particular attribute and a related control, in that in some companies one control serves to support several attributes, and in other companies multiple controls are needed to support one attribute.

A company may use one or more of the approaches described, or take another approach better suited to its culture, management style and processes in applying a principle. Although the descriptions of many of the approaches speak in terms of management being directly involved in carrying out the approach, in many instances tasks are delegated to other personnel.

Examples

Examples illustrate how the approaches can be used to apply the principle. As with the approaches, each example is referenced to related attributes, which may be useful in considering how best to achieving the principle. The examples are set forth in the context of a particular company, with most being drawn from actual businesses.

The examples are provided for illustrative purposes so that management may consider applicability, and are not intended to be construed as "best practices" or suggested solutions for

all users of this guidance. Users should recognize that because the examples are limited in scope, they are not necessarily sufficient with respect to a particular approach or related attribute(s) or principle.

Approaches will be somewhat different in different organizational environments and, and for a particular company are likely to evolve as circumstances change. Accordingly, while the principles are expected to remain constant, approaches taken to apply the principles may be temporal.

Determining Effectiveness

Whether designing and implementing or conducting an assessment of internal control over financial reporting, this material is designed to help management of smaller businesses determine whether the internal control components are in place and operating effectively such that the company has reasonable assurance that it will prevent or detect material misstatements on a timely basis. Ultimately, management needs to evaluate the company's internal control system in relation to the *Framework*. The criteria for effectiveness – being the presence and effective functioning of each of the five components – are established in the *Framework*, and that document remains the definitive reference for determining effectiveness of internal control.

Because the twenty principles contained in this guidance are drawn directly from the *Framework*'s components, a company – even a smaller one – can achieve effective internal control by applying all of the underlying principles.

When a principle is not being met, an internal control deficiency exists. Such deficiencies should be evaluated to determine whether they rise to the level of significant deficiency or material weakness in deciding what action to take and ultimately making a determination on internal control effectiveness.

At the end of this volume is a diagram to assist management in navigating this guidance. This diagram integrates the discussion on viewing internal control as a process with the twenty principles and supporting attributes to assist management in determining the effectiveness of internal control.

Conclusion

Smaller businesses have unique challenges in achieving effective internal control, but the challenges are manageable. This guidance provides insights to assist management of smaller companies minimize incremental costs associated with internal control design, implementation and assessment, so that the benefits of reliable financial reporting and access to public capital markets continue to exceed the cost of control.

This guidance, however, does not provide "relief" in the form of a short cut to achieving effective internal control over financial reporting. The *Framework* is integrated, designed such that each of the components contributes to internal control effectiveness and must be present and operating effectively. This guidance points out, however, how some tradeoffs among and within components may appropriately be made. Judgment is applied in determining whether a company's particular component configuration is sufficient to achieve effective internal control.

Stakeholders are best served when company management resist any temptation to balance costs and benefits of internal control by reducing internal control effectiveness, instead recognizing and embracing the significant benefits of effective internal control investments beyond mere compliance. These benefits generally can be achieved in a truly cost-effective manner.

I. Control Environment

The control environment component is the foundation upon which all other components of internal control are based, and sets the tone of an organization.

A smaller company can have unique advantages in establishing a strong control environment. Employees in many smaller businesses interact more closely with top management and are directly influenced by management actions. Through day-to-day practices and actions, management can effectively reinforce the company's fundamental values and directives. The close working relationship also enables senior management to recognize quickly where employees' actions need modification.

Seven principles relate to the control environment component:

1. **Integrity and Ethical Values** – Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.
2. **Board of Directors** – The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.
3. **Management's Philosophy and Operating Style** – Management's philosophy and operating style support achieving effective internal control over financial reporting.
4. **Organizational Structure** – The company's organizational structure supports effective internal control over financial reporting.
5. **Financial Reporting Competencies** – The company retains individuals competent in financial reporting and related oversight roles.
6. **Authority and Responsibility** – Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.
7. **Human Resources** – Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.

Guidance useful in designing and implementing or assessing application of the principles is provided in the balance of this chapter, with additional illustrative guidance included in Volume III.

Principle 1
Integrity and Ethical Values

Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.

Attributes of the Principle

Articulates Values – Top management develops a clearly articulated statement of ethical values that is understood at all levels of the organization.

Monitors Adherence – Processes are in place to monitor adherence to principles of sound integrity and ethical values.

Addresses Deviation – Deviations from sound integrity and ethical values are identified in a timely manner and appropriately addressed and remedied at appropriate levels within the company.

Approaches to Applying the Principle

Articulating and Demonstrating Integrity and Ethics

Articulates Values
Monitors Adherence
Addresses Deviation

The CEO and key members of management articulate and demonstrate the importance of sound integrity and ethical values to employees through their:

- Day-to-day actions and decision making.
- Interactions with suppliers, customers, and other external parties that reflect fair and honest dealings.
- Performance appraisals and incentives that diminish temptations inconsistent with financial reporting objectives.
- Intolerance of ethical violations at all levels.

Informing Employees about Integrity and Ethics

Articulates Values
Monitors Adherence
Addresses Deviation

Management implements mechanisms to inform new employees and remind current personnel of the company's objectives related to integrity and ethics and related corporate values. Such mechanisms include:

- Providing information to new hires emphasizing top management's views about the importance of sound integrity and ethics.
- Periodically providing employees updated information relevant to maintaining sound integrity and ethical values.
- Making ethics guidelines readily available and understandable.

- Including periodic training or other interactive communications to review current and new ethics policies.
- Periodically receiving confirmations from employees on their understanding of key principles.
- Recognizing and rewarding employees' actions that positively reflect sound integrity and ethical values.

Demonstrating Commitment to Integrity and Ethics

Articulates Values
Monitors Adherence
Addresses Deviation

Management demonstrates its commitment to sound integrity and ethical values by following a prescribed investigation process and taking appropriate, timely corrective action when possible violations are identified. For example, management:

- Investigates occurrences of possible violations to gain a thorough understanding of issues and circumstances.
- Develops appropriate documentation.
- Remedies the situation in accordance with prescribed company guidelines on a consistent and timely basis.
- Makes company personnel aware that appropriate investigation and corrective actions have been taken.
- Follows up to support continued compliance.

Examples of Applying the Principle

Company Newsletter Reinforcing Integrity and Ethics

Articulates Values
Monitors Adherence
Addresses Deviation

A supplier to the aerospace industry emphasizes the importance of exercising sound integrity and ethical values in its monthly newsletter to employees. Each newsletter contains a section related to ethical decision making, emphasizing key aspects of the company's mission statement and ethical values and including examples of ethical dilemmas with suggested resolutions. The newsletter reminds all employees that as part of their annual performance review they must certify that they have read the company's mission statement and code of conduct and that they are in compliance with those policies.

Promoting Awareness of Ethical Behavior

Articulates Values
Monitors Adherence
Addresses Deviation

A 650-person construction materials company promotes awareness of its expectations for ethical behavior as a part of regularly scheduled employee meetings. Key components of the code of conduct are discussed, with key points captured for reinforcement in written communications.

Aligning Incentives with Ethics and Values

Articulates Values
Monitors Adherence
Addresses Deviation

A 250-employee forest products company structures its bonus plan to have 30% of the potential incentive award directly related to demonstration of the company's core values. Specific comments on how management does or does not reflect values are captured through upward feedback mechanisms. During the employee performance review and appraisal process, management provides feedback about the extent to which each employee has performed in accordance with the company's core values of sound integrity and ethics.

Promoting a Commitment to Ethics

Articulates Values
Monitors Adherence
Addresses Deviation

A designer and marketer of men's and women's sportswear with $125 million annual revenue promotes its commitment to ethical behavior through making its code of conduct readily available to all employees and third parties on its website, and requiring employees to review the code and sign a confirmation stating whether he/she has read it and is in compliance with its provisions. The code of conduct contains clear information on how to report a policy violation through an independent third party.

Promoting Employee Participation in Identifying Misconduct

Articulates Values
Monitors Adherence
Addresses Deviation

A food distribution company with $400 million annual revenue promotes reporting of misconduct by providing an anonymous help line for its 600 employees to report potential fraud occurrences and other ethical concerns, without fear of reprisal. The company engages a third-party service provider to proctor the help line. Potentially illegal acts or financial reporting improprieties reported through the help line are communicated directly to the general counsel and audit committee.

Taking Actions When Deviations Occur

Articulates Values
Monitors Adherence
Addresses Deviation

A shoe company with 14 locations established a policy addressing serious improprieties, where in specified circumstances (cash embezzlement, for example) the employee's access privileges to the facilities and IT systems are suspended temporarily and a full investigation launched. Where the impropriety is confirmed, the company terminates the employee, permanently revokes all access privileges, and files formal charges with appropriate authorities. After documenting the situation and its resolution, the HR manager is required to analyze the underlying root causes, and implement any additional remedial steps needed to avoid similar occurrences.

Principle 2
Board of Directors

The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.

Corporate governance has evolved such that audit committees perform most of the activities noted below. Increasingly, boards of smaller companies have audit committees of independent directors. When a board chooses not to have an audit committee, the full board performing the activities described should have a sufficient number of independent members.

Attributes of the Principle

Defines Authorities – The board defines and communicates authorities retained at the board level and those delegated to management.

Operates Independently – The board has a critical mass of members who are independent directors.

Monitors Risk – The audit committee actively evaluates and monitors risks of management override of internal control and considers risks affecting the reliability of financial reporting.

Retains Financial Reporting Expertise – One or more audit committee members has financial reporting expertise.

Oversees Quality and Reliability – The audit committee provides oversight to the effectiveness of internal control over financial reporting and financial statement preparation.

Oversees Audit Activities – The audit committee oversees the work of both internal and external auditors, and interacts with regulatory auditors if necessary. The audit committee has exclusive authority to engage, replace, and determine the compensation of the external audit firm. The audit committee meets privately with internal and external audit to discuss relevant matters.

Approaches to Applying the Principle

In many instances the following approaches may be performed by an audit committee of the board, communicating key issues to the board.

Establishing Content for Board Meetings

The board of directors establishes a formal policy for specific decisions or events that require discussion with or approval from the board, as well as a calendar for the timing of these discussions.

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

Identifying Independent Board Members

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The board of directors identifies independent board and audit committee members through sources available to smaller businesses:

- The American Institute of Certified Public Accountants maintains a list of certified public accountants interested in board and audit committee membership.
- Financial Executives International also maintains a list of potential directors.
- The National Association of Corporate Directors maintains a similar list.
- Many retired public accounting firm partners and chief internal auditors express interest in directorships.
- Accounting academicians, a largely untapped resource, can add value as directors.
- Controllers and CFOs of other smaller companies as well as larger organizations can serve as effective board and audit committee members.

Establishing Boards Roles and Responsibilities

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The board of directors through the corporate bylaws, and the audit committee through its charter, set forth their roles and responsibilities.

Audit Committee Considering Effectiveness of Internal Control

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The audit committee regularly considers the effectiveness of internal control over financial reporting, including risks, significant deficiencies, and material weaknesses (if any).

Audit Committee Meeting with Auditors

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The audit committee meets regularly with the internal and external auditors, including in private meetings. The committee reviews audit scope and testing plans, resources and staffing, and significant audit findings.

Audit Committee Reviewing Policies and Procedures

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The audit committee reviews accounting policies and procedures used by management for determining significant estimates, including key assumptions.

Audit Committee Maintaining Skepticism

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The audit committee maintains an appropriate level of skepticism regarding management's assertions and judgments affecting financial reporting, asking probing and challenging questions of management.

Audit Committee Considering Whistle-blower Information

The audit committee considers information obtained from the whistle-blower program and the company's anti-fraud and similar processes to monitor the risks of misstatements in financial reporting, including risks of inappropriate acts by staff and management override of controls. The committee reviews reports of significant matters, considering the potential impact on financial reporting and need for corrective action.

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

Board Reviewing Audit Committee Candidates

The board conducts due diligence on board and audit committee candidates to confirm appropriate independence from the company and management and his/her ability to be an effective board member. Such procedures include:

- Performing background checks.
- Obtaining independent references.
- Reviewing current affiliations/directorships.
- Reviewing information about financial and other relationships with the company, its external auditors, or management.
- Using an independent nominating committee or search firm to oversee due diligence procedures.
- Monitoring performance of due diligence procedures by independent directors.

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

Audit Committee Certifying Compliance

Audit committee members certify annually their compliance with the company's ethics guidelines and independence rules.

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

Board and Audit Committee Meeting with Management

The board of directors and audit committee allocate a portion of every meeting for discussions of issues without management present, including separate time with external advisors, internal audit, the external auditor and outside legal counsel.

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

Examples of Applying the Principle

Reviewing and Documenting Key Activities of the Board

The audit committee of an electricity distributor reviews performance reports against budgets and management's explanations for significant variances, and participates in approving major business decisions such as acquisitions, major capital expenditures, and bonus and incentive arrangements. The committee engages the external auditor, reviews audit plans, reviews management's assessment of internal control over financial reporting, and is apprised by management on a timely basis of the company's approach for adopting new accounting standards that significantly impact financial reporting. Annually, the committee performs a self-assessment of its performance.

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

Audit Committee's Independence and Financial Reporting Expertise

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

A manufacturer of lighting and ventilation equipment with annual revenues of $115 million has an audit committee with three independent members. The company's audit committee uses its charter in setting its meeting agendas. For each of the committee's responsibilities set forth in the charter, the audit committee chair identifies at least one audit committee meeting during the year at which the matter is to be discussed.

The audit committee chair possesses financial reporting expertise (she is a CPA and has previous public accounting experience). She submits draft agendas for upcoming meetings to other committee members and the external auditors seeking feedback on the need for additional agenda items. The audit committee chair has developed an open channel for candid and ongoing dialogue with the external audit engagement partner.

Reviewing Financial Statement Estimates

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The audit committee of a $200 million manufacturer of specialty polymer products meets regularly with management to discuss assumptions used by management related to key financial statement accounts and disclosures. The committee reviews the reasonableness of management's assumptions and judgments used to develop significant estimates, and meets privately with the external auditor to discuss its assessment of management's estimates and the related impact on financial reporting.

Audit Committee Interacting with External Auditors

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

Management of a marine construction services provider meets with the external auditor quarterly, and in executive session (without management present) at least annually, to discuss a wide range of issues such as audit scope, testing plans, internal control over financial reporting, quality of financial reporting, and audit findings and recommendations. Through these interactions, supplemented as needed with interim conversations, the audit committee chair believes the committee is well positioned to monitor the external auditor's performance and make an informed judgment on any need to modify or terminate the relationship.

Audit Committee Considering the Potential of Management Override

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

The audit committee of an electricity transmission and distribution company discusses in executive session at least annually its assessment of the risks of management override of internal control, including motivations for management override and how those activities might be concealed. The committee reviews the functioning of the company's whistle-blower process and related reports, and from time to time inquires of managers not directly responsible for financial reporting (including personnel in sales, procurement, and human resources, among others), obtaining information regarding any concerns about ethics or indications of management override of internal controls.

Changing Board Composition of Closely-Held Company

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

A mining exploration company whose shares are traded on an "over-the-counter" bulletin board has long maintained a board of directors that included three of the CEO's family members and three outside but not independent directors – the company's outside counsel, a venture capitalist, and a personal friend of the CEO.

To strengthen the control environment and board's effectiveness, the board was reconstituted as follows: The relatives and personal friend of the CEO left the board and three independent directors

were added, all financially literate with one possessing financial expertise. The three independent directors were appointed to a newly formed audit committee with its responsibilities set forth in a charter.

Audit Committee Setting Agendas

The audit committee of an aerospace control systems supplier establishes a calendar of topics for the coming fiscal year. This helps the audit committee cover all relevant responsibilities, and helps management anticipate and plan for the committee's expectations.

Defines Authorities
Operates Independently
Monitors Risk
Retains Financial Reporting Expertise
Oversees Quality and Reliability
Oversees Audit Activities

	Frequency			Planned Meeting Quarter			
	A	E	AN	1	2	3	4
Audit Committee Issues							
Report of results of annual independent audit to the board	✓			✓			
Appointment of the external auditor	✓			✓			
Approval of external auditor fees for upcoming year				✓			
Review of annual proxy statement audit committee report	✓			✓			
Assessment of the adequacy of audit committee charter	✓				✓		
Approval of audit committee meeting plan for the upcoming year, confirm mutual expectations with management and the auditor	✓				✓		
Audit committee self-assessment					✓		
Approval of guidelines for engagements of external auditors for other services (pre-approval policy)	✓			✓			
Approval of any non-audit services provided by outside auditors			✓				
Report of external auditor pre-approval status/limits		✓		✓	✓	✓	✓
Review of procedures for handling financial reporting errors or irregularities	✓				✓		
Oversees fraud risk assessment process	✓			✓			
Approval of minutes of previous meeting		✓		✓	✓	✓	✓
Report quarterly matters to the board (chair)		✓		✓	✓	✓	✓
Schedule executive session of committee members			✓				
Other matters			✓				
Financial Management							
Annual Report, 10-K, and Proxy Statement Matters	✓			✓			
Quarterly report earnings review with management and external auditor, pre-approval of external auditor professional activities		✓		✓	✓	✓	✓
Assessment of system of internal control	✓			✓			
Status of significant accounting estimates, judgments and special issues (e.g. major transactions, accounting changes, SEC issues, etc.)			✓				
Other matters (adequacy of staffing, succession planning, etc.)			✓				

A = Annually E = Each Meeting or Conference Call AN = As Necessary

(continued next page)

Audit Committee Setting Agendas (continued)

	Frequency			Planned Meeting Quarter			
	A	E	AN	1	2	3	4
Other Members of Management							
Legal matters (General Counsel)			✓				
Conflict of interest and ethics policies	✓				✓		
Litigation status/regulatory matters			✓				
Information systems matters (IT Manager)			✓				
Risk Management Manager			✓				
Tax matters (Tax Manager)			✓				
Others			✓				
External Auditor							
Results of annual audit including required communications	✓			✓			
Results of timely quarterly reviews including required communications		✓		✓	✓	✓	✓
Report on internal control weaknesses and other recommendations and management response, if applicable			✓				
Scope of annual audit	✓			✓			
Required written communication and discussion of independence (SAS 61 & ISBS 1)	✓			✓			
Other matters (succession planning, etc.)			✓				
Executive session with external auditor			✓				
Internal Auditor							
Scope of internal auditing plan for upcoming year	✓						✓
Coordination with external auditor /outsource auditor			✓				
Defalcations and irregularities – whistle-blower hotline activity		✓		✓	✓	✓	✓
Summary of significant audit findings and status update relative to annual plan		✓		✓	✓	✓	✓
Executive session with internal audit risk assessment			✓				

A = Annually E = Each Meeting or Conference Call AN = As Necessary

Principle 3
Management's Philosophy and Operating Style

Management's philosophy and operating style support achieving effective internal control over financial reporting.

Attributes of the Principle

Sets the Tone – Management's philosophy and operating style emphasize reliable financial reporting.

Influences Attitudes towards Accounting Principles and Estimates – Management's attitude supports a disciplined, objective process in selecting accounting principles and developing accounting estimates.

Articulates Objectives – Management establishes and clearly articulates financial reporting objectives, including the role of internal control over financial reporting.

Approaches to Applying the Principle

Emphasizing Risk Mitigation

Management emphasizes the importance of minimizing risks related to financial reporting in its interactions with others involved in the financial reporting process, and through its dealings with customers, suppliers or distributors, and employees.

Sets the Tone
Influences Attitudes towards Accounting Principles and Estimates
Articulates Objectives

Emphasizing Processing Requirements

The company's operating philosophy requires that all journal entries, including those reflecting assumptions and estimates, be properly authorized, supported by adequate documentation and subject to review by an appropriate senior financial executive.

Sets the Tone
Influences Attitudes towards Accounting Principles and Estimates
Articulates Objectives

Emphasizing Importance of Diligence

Management provides sufficient direction such that employees recognize the importance of applying appropriate diligence and business judgment in the performance of assigned job responsibilities.

Sets the Tone
Influences Attitudes towards Accounting Principles and Estimates
Articulates Objectives

Establishing and Articulating Financial Reporting Objectives

Sets the Tone
Influences Attitudes towards Accounting Principles and Estimates
Articulates Objectives

Management establishes and articulates financial reporting objectives, including those relating to complete, accurate and fair financial reporting, with personnel involved in the financial reporting process.

Examples of Applying the Principle

Reinforcing the Tone for Effective Financial Reporting

Sets the Tone
Influences Attitudes towards Accounting Principles and Estimates
Articulates Objectives

Management of an online marketing services provider with $170 million annual sales takes steps to manage risks associated with the company's aggressive approach to managing the business to achieve the company's short-term goals. In order to minimize opportunities for inappropriate financial reporting, senior management actively monitors the actions of operating managers, utilizes the services of an outsourced internal audit firm to review high risk activities, and reminds employees through ongoing oral communications and reinforced with their own business conduct that unethical behavior will not be tolerated.

Soliciting Suggestions for Enhanced Internal Control

Sets the Tone
Influences Attitudes towards Accounting Principles and Estimates
Articulates Objectives

A company in the research, development, production, and marketing of medical scanning equipment encourages its 495 employees to submit suggestions for improvements in internal control, including internal control over financial reporting. Employees are rewarded for ideas that are used.

Emphasizing Philosophy with External Parties

Sets the Tone
Influences Attitudes towards Accounting Principles and Estimates
Articulates Objectives

As part of its standard contracting processes with customers and other parties, a provider of temporary staffing to service and technology companies highlights in its standard contract the company's commitment to excellence and ethical conduct. The contract encourages external parties to notify the company's general counsel if suspicions arise about questionable employee actions, with clear communications procedures provided.

Principle 4
Organizational Structure

The company's organizational structure supports effective internal control over financial reporting.

Attributes of the Principle

Establishes Lines of Financial Reporting – Management establishes appropriate lines of financial reporting for each functional area and business unit in the organization.

Establishes Structure – Management maintains an organizational structure that facilitates effective reporting and other communications about internal control over financial reporting.

Approaches to Applying the Principle

Developing Organizational Charts

Management develops an organizational chart, which sets forth roles and respective reporting lines for all employees, including those involved in financial reporting.

Establishes Lines of Financial Reporting
Establishes Structure

Aligning Roles to Processes

Each unit or function within the organization aligns roles to key processes supporting financial reporting objectives.

Establishes Lines of Financial Reporting
Establishes Structure

Maintaining Job Descriptions

Management maintains job descriptions for key positions and updates them as conditions and circumstances warrant.

Establishes Lines of Financial Reporting
Establishes Structure

Establishing Organizational Structures

Management adopts a structure whereby the there are only three staff layers between the CFO and personnel directly involved in the financial reporting process.

Establishes Lines of Financial Reporting
Establishes Structure

Establishing Structure for Internal Audit

An internal audit function reports directly to the CEO, with direct assess to the audit committee, to maintain independence over financial reporting.

Establishes Lines of Financial Reporting
Establishes Structure

Examples of Applying the Principle

Establishing Job Descriptions and Responsibilities

Establishes Lines of Financial Reporting
Establishes Structure

The CEO of a supplier of replacement parts to the automotive aftermarket requires each business unit manager to maintain up-to-date written job descriptions for each position in the business unit. Organization charts are maintained and periodically updated depicting positions and lines of reporting within the unit.

Reorganizing to Support Control Structure

Establishes Lines of Financial Reporting
Establishes Structure

Before a $130 million real estate company became public, a wide range of employees reported to the owner and CEO. With plans to go public, the CEO with the board's guidance took steps to strengthen the organizational structure to better support both operations and financial reporting objectives. Management created three departments – sales and customer service, purchasing/inventory, and production – to oversee its core business activities. Managers leading each of these departments, as well as managers of key staff functions, reviewed existing internal controls, strengthening them as necessary. The business processes were documented to highlight key risks and related controls and each person's responsibility in the processes. Job descriptions including internal control responsibilities were developed to support full understanding of each person's role. In addition to these structural improvements, the CEO sought to continue what long was an open culture, assuring employees that an "open door" policy exists, designed to encourage the free flow of information throughout the organization.

Principle 5
Financial Reporting Competencies

The company retains individuals competent in financial reporting and related oversight roles.

Attributes of the Principle

Identifies Competencies – Competencies that support reliable financial reporting are identified.

Retains Individuals – The company employs or otherwise retains individuals who possess the required competencies related to financial reporting.

Evaluates Competencies – Needed competencies are regularly evaluated and maintained.

Approaches to Applying the Principle

Establishing Required Knowledge, Skills and Abilities

Before hiring for key financial positions, management establishes and agrees on the knowledge, skills, and abilities (and related credentials) needed to effectively carry out the associated responsibilities.

Identifies Competencies
Retains Individuals
Evaluates Competencies

Supplementing Competencies

The company supplements in-house financial reporting competencies as needed by establishing arrangements with outside specialists.

Identifies Competencies
Retains Individuals
Evaluates Competencies

Providing Training

Management provides training for employees involved in financial reporting processes, either in-house or through outside service providers.

Identifies Competencies
Retains Individuals
Evaluates Competencies

Evaluating Competencies in Key Financial Reporting Roles

The board of directors or audit committee evaluates the competencies of individuals serving in key financial reporting roles, such as CEO and CFO.

Identifies Competencies
Retains Individuals
Evaluates Competencies

Reviewing and Evaluating Competencies

Management periodically reviews and evaluates employees relative to their assigned roles to determine whether the employees' skills are appropriate for their current job responsibilities.

Identifies Competencies
Retains Individuals
Evaluates Competencies

Examples of Applying the Principle

Utilizing Outside Service Provider

Identifies Competencies
Retains Individuals
Evaluates Competencies

A 500-person company that provides identify-theft protection and credit management services to credit card companies considered whether to perform payroll and 401(k) plan administration in-house or have them done by an outside service. It was determined there is a significant economic benefit to having an outside service perform these functions, and use of the third party improves segregation of duties and enhances access to qualified specialists. Having engaged a service, the company now regularly obtains and considers SAS 70 internal control reports issued by the service's auditor to evaluate whether appropriate controls are in place.

Aligning Competency with Key Financial Reporting Positions

Identifies Competencies
Retains Individuals
Evaluates Competencies

The human resources vice president of a $140 million provider of wireless data communications solutions annually reviews employee job descriptions and performance assessments, and together with knowledge of evolving corporate needs determines whether employee competencies continue to be aligned with roles and responsibilities. With revenue having doubled over the last several years, it was determined that because of greater complexity in business transactions and processing the company's controller, hired initially to perform basic accounting and bookkeeping functions, no longer had the expertise needed for the associated financial reporting responsibilities. The company assigned the controller to a position better suited to his skills, and hired an individual with the requisite competencies as controller.

Retaining External Tax Assistance

Identifies Competencies
Retains Individuals
Evaluates Competencies

A $160 million developer of analytical software products does not have an individual with strong tax accounting expertise on staff. To support the VP, Finance, who with a basic knowledge of tax accounting prepares a preliminary income tax provision, the company retains a third party accounting firm (not its auditor) to review the provision. Management is comfortable that the third party accounting firm has the proper skills and staff assigned to do this work. After any necessary changes are made pursuant to the accounting firm's review, the company's CFO reviews the tax provision and compares the results to expectations based on past periods, budgets and knowledge of business operations.

Assessing Key Financial Reporting Personnel

Identifies Competencies
Retains Individuals
Evaluates Competencies

Annually, a $180 million investment bank and institutional securities company undertakes a process to assess the ability of its key financial reporting personnel to deal effectively with the company's current business activities. Leveraging the knowledge of its external auditor gained through its interaction with members of the financial organization and with participation of the audit committee chair, management considers the competencies, skill sets, and performance of the key members of the financial reporting team and based on this assessment makes decisions on staff training, reassignments or other changes.

Principle 6
Authority and Responsibility

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.

Attributes of the Principle

Defines Responsibilities – Assignment of responsibility and delegation of authority are clearly defined for all employees, including:

- *Board* – The audit committee oversees management's process for defining responsibilities for key financial reporting roles.
- *Top Management* – The CEO and top management are responsible for sound internal control over financial reporting, including both initiating and maintaining the internal control system.
- *Senior and Functional Management* – Senior and functional management are responsible for ensuring all employees understand their responsibilities for achieving financial reporting objectives through adherence to internal control policies and procedures.

Limits Authority – Assignment of authority and responsibility includes appropriate limitations.

Approaches to Applying the Principle

Defining Objectives and Responsibilities

Management sets forth clear business and management objectives and position descriptions to reinforce management's responsibility for effective internal control over financial reporting.

Defines Responsibilities
Limits Authority

Audit Committee Reviewing Key Positions

For key financial reporting positions, the audit committee reviews management's descriptions of the positions' responsibilities and authorities, and considers how those positions affect the strength of internal control over financial reporting, calling for reevaluation where needed.

Defines Responsibilities
Limits Authority

Assigning Authorities and Responsibilities

In assigning authorities and responsibilities, management considers the impact on the effectiveness of the control environment and importance of maintaining effective segregation of duties. Management establishes an appropriate balance between the authority needed to "get the job done" and the need to maintain adequate internal control over key processes.

Defines Responsibilities
Limits Authority

Empowering Employees

Defines Responsibilities
Limits Authority

Management empowers employees to correct problems or implement improvements in their assigned business processes as necessary, balanced with appropriate monitoring of performance.

Aligning Positions with Responsibilities and Authorities

Defines Responsibilities
Limits Authority

Management considers the nature of employee positions within the organization when assigning responsibilities to individuals or determining certain levels of authority for positions.

Examples of Applying the Principle

Audit Committee Review of Managers' Roles

Defines Responsibilities
Limits Authority

A $115 million lead products company's bylaws explicitly specify board responsibility for reviewing the principal roles and responsibilities of key financial reporting management. This is achieved by the audit committee chair meeting annually with the company's human resource director, chief internal auditor, legal counsel, and external auditor to review the managers' roles, responsibilities and performance. The review includes focus on alignment of respective responsibilities with the company's organization chart and the managers' expertise and experience in carrying out the responsibilities.

Reviewing and Approving Internal Audit Plan

Defines Responsibilities
Limits Authority

Annually, a real estate company's internal audit director presents to the CEO, CFO and audit committee for review and approval internal audit's scope, work plan, staffing and budget for the coming year, as well as any needed modification in its charter defining role and responsibilities.

Top Management Reorganizing Reporting Lines

Defines Responsibilities
Limits Authority

Senior management of a 400-person games software developer recognized that with recent significant growth the roles and responsibilities for its management executives were no longer relevant. Overlap existed in responsibilities of the controller and CFO, systems for product being sold through new channels were not adequately reviewed, and information on new initiatives and agreements known by the CEO were not being communicated clearly and timely across the senior management team. A project was initiated to realign responsibilities among its leadership team to adequately support financial reporting objectives, with clear lines of reporting supported by new written job descriptions.

CEO and Board Input to Developing Roles

Defines Responsibilities
Limits Authority

Due to significant changes within the company and the industry, the CEO of a transportation services provider set an initiative to redefine the role of each position within the company's mid- to high-level management team. An off-site meeting was held where goals and objectives of the business were reviewed and realigned with managers' specific roles and responsibilities, including those related to the financial reporting process. Two board members were present, serving as a sounding board, with all participants coming to a shared understanding on how they will function and interact with one another going forward. The result was communicated to other managers throughout the organization, with a description of organization lines, responsibilities and communication procedures incorporated into policies readily accessible on the company's intranet.

Management Assigning Levels of Authority

Management of a $120 million home construction company with 565 employees structures the finance department and assigned levels of authority and responsibility for specific positions based on need and skills. A personnel organization chart depicts the assigned responsibilities at all levels and references written job descriptions for all employees. Employees are evaluated based on the performance of those responsibilities.

Defines Responsibilities
Limits Authority

Principle 7
Human Resources

Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.

Attributes of the Principle

Establishes Human Resource Practices – Management establishes human resource practices that demonstrate its commitment to integrity, ethical behavior, and competence.

Recruits and Retains – Employee recruitment and retention for key financial reporting positions are guided by principles of integrity and by necessary competencies associated with the positions.

Adequately Trains – Management supports employees by providing tools and training needed to perform their financial reporting roles.

Evaluates Performance and Compensates – Employee performance evaluations and the company's compensation practices, including those affecting top management, support achievement of financial reporting objectives.

Approaches to Applying the Principle

Developing and Maintaining Position Descriptions

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Management develops and maintains position descriptions that reflect its values and the competencies needed to execute position requirements.

Developing and Maintaining Human Resource Policies and Procedures

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

The human resource function develops and periodically updates materials outlining the company's human resource policies and procedures.

Reviewing Resumes and Performing Reference Checks

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Management reviews resumes and performs reference checks in considering candidates for key financial reporting positions. For positions with high level responsibility and authority, the company also performs background checks.

Providing Training and Awareness

The human resource function provides training and awareness programs to promote ethical behavior throughout the organization. Additional training programs related to financial reporting are provided to all employees with direct and indirect involvement in financial reporting.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Establishing a Review and Appraisal Process

Management establishes a review and appraisal process that confirms knowledge of each employee's progress and status within the organization.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Performing Exit Interviews

A company's process for performing exit interviews includes inquiries about any concerns related to the company's financial reporting and internal control.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Designing Compensation Plans

Compensation plans for senior executives include a significant element tied to achievement of non-financial goals (for example, customer satisfaction, employee retention, and successful systems implementation) and is not excessively tied to short-term results as reflected in financial statements.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Reviewing Compensation Plans

The board reviews management compensation plans, including bonus and stock compensation components, to determine whether the plans create inappropriately high risk of financial reporting misstatements and implements controls as needed to reduce risk to an acceptable level.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Evaluating Competency of Personnel

Management evaluates the sufficiency and competency of personnel involved in recording and reporting financial information. Top management assesses their ability to identify issues, articulate positions supported by relevant literature and stay abreast of new technical financial reporting developments. Considerations when assessing the adequacy and competency of financial reporting personnel include overall technical skills, nature and frequency of their training, and the number of personnel dedicated to financial reporting.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Examples of Applying the Principle

Developing Human Resource Practices

An Internet and catalog retailer of upscale gifts without a full-time human resource professional formed a task force of several managers to develop human resource practices and policies. The policies were reviewed by senior management and the board, and implemented by line management.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Periodically Reviewing Policies

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

The human resources leader of a 350-employee provider of networking technology platforms periodically reviews HR policies and effectiveness, including the means by which they are disseminated throughout the organization. The content, relevance, timeliness, and level of understanding by employees are included within the review. Newly hired employees receive the current version of the company's policies and procedures, and other employees receive updated policies when issued. Surveys are conducted periodically to assess the extent to which employees are aware of the most recent versions of the policies, with the results used to track progress and shape program enhancements.

Recruiting and Retaining Key Financial Reporting Positions

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

The CFO of a garage door manufacturer with $250 million revenue sought a controller for its affiliate in France with strong capabilities for the position, including in-depth US public filing reporting compliance requirements and high levels of integrity and sound ethical values. The organization preferred avoiding the cost of an outside search firm, and instead identified a successful candidate through international professional organizations (including FEI and IIA France). Candidate screening included interviews with a cross section of leaders of key functional areas of the business followed with the CFO interviewing the candidate's references. In order to successfully recruit this well-qualified candidate, in addition to competitive salary and benefits, the company included in the position description the opportunity to attend two weeks annual professional educational programs.

Evaluating Integrity and Ethics in the Hiring Process

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

In interviewing prospective employees, the human resources leader of a $175 million gas utility focuses significant attention to matters relating to personal integrity and ethical values, with in-depth interviews and background screening. All new employees are provided a copy of the company's code of conduct, and subsequently are required to sign off that they have received and read the code.

Providing Adequate Technical Training

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

A $180 million chemical company sends three managers to external specialized training. The managers subsequently hold an on-site training session for the employees in their respective departments. This approach allows the organization to receive relevant, up-to-date technical accounting information in a cost-effective manner. Additionally, other course offerings and descriptive outlines of training programs are made available to all employees so they are aware of company-supported training opportunities. Documentation of training attended is tracked and included in employee files.

Implementing Complex Accounting Standards

A mining exploration company makes extensive use of stock options in compensating its senior employees. The company has one individual filling the roles of both CFO and controller. Although generally competent in applying most elements of GAAP, this individual is not sufficiently knowledgeable in applying a recently-issued pronouncement on accounting for stock compensation. Management considered outsourcing initial implementation of the new standard to a third-party expert, but decided it could accomplish its objective more cost-effectively by providing training to the CFO/controller to develop the needed competencies. With input provided by the external auditor, management was comfortable that the CFO/controller had sufficient knowledge to make informed decisions on proper application of the standard.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Training Through Professional Organizations

A CFO from an $80 million venture capital company attends continuing professional education sessions. She is required by her professional organization to attend 35 hours per year, and targets her attendance to those sessions most relevant to her day-to-day responsibilities. Attendance certificates provided by her organization evidence such training.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

Periodically Assessing Performance

A New York-based provider of satellite communication solutions with $110 million annual sales periodically reviews the performance of employees responsible for owning, executing, or testing financial reporting controls. Performance is evaluated against expectations established at the beginning of the year, with progress on needed improvements reviewed with employees at the end of each quarter and a more formal annual review process following the year-end reporting cycle.

Establishes Human Resource Practices
Recruits and Retains
Adequately Trains
Evaluates Performance & Compensates

II. Risk Assessment

Risk assessment as it relates to the objective of reliable financial reporting involves identification and analysis of the risks of material misstatement.

Establishment of financial reporting objectives articulated by a set of financial statement assertions for significant accounts is a precondition to the risk assessment process. Risk assessment in smaller companies can be relatively efficient, often because in-depth knowledge of the company's operations enables the CEO and other senior managers to have first-hand information of where risks lay. In carrying out their normal responsibilities, including obtaining information gained from employees, customers, suppliers and others, these managers identify risks inherent in business processes. In addition to focusing on operations and compliance risks, they are positioned to consider such risks to reliable financial reporting as:

- Failing to capture and record all transactions
- Recording assets that do not exist or transactions that did not occur
- Recording transactions in the wrong period or wrong amount, or misclassifying transactions
- Losing or altering transactions once recorded
- Failing to gather pertinent information to make reliable estimates
- Recording inappropriate journal entries
- Improperly accounting for transactions or estimates
- Inappropriately applying formulas or calculations.

Three principles relate to risk assessment:

8. **Financial Reporting Objectives** – Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.
9. **Financial Reporting Risks** – The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.
10. **Fraud Risk** – The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

Guidance useful in implementing or assessing the application of the principles is provided in the balance of this chapter, with additional illustrative guidance included in Volume III.

Principle 8
Financial Reporting Objectives

Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.

Attributes of the Principle

Complies with Generally Accepted Accounting Principles – Financial reporting objectives are consistent with generally accepted accounting principles. The accounting principles selected are appropriate in the circumstances.

Supports Informative Disclosures – Financial statements are informative of matters that may affect their use, understanding, and interpretation. Information presented is classified and summarized in a reasonable manner, neither too detailed nor too condensed.

Reflects Company Activities – The financial statements reflect the underlying transactions and events in a manner that presents the financial position, results of operations, and cash flows within a range of acceptable limits.

Are Supported by Relevant Financial Statement Assertions – Supporting the objectives is a series of financial statement assertions that underlie a company's financial statements, with relevance depending on circumstances.

- *Existence* – Assets, liabilities, and ownership interests exist at a specific date, and recorded transactions represent events that actually occurred during a certain period.
- *Completeness* – All transactions and other events and circumstances that occurred during a specific period, and should have been recognized in that period, have been recorded.
- *Rights and Obligations* – Assets are the rights, and liabilities are the obligations, of the entity at a given date.
- *Valuation or Allocation* – Asset, liability, revenue, and expense components are recorded at appropriate amounts in conformity with relevant and appropriate accounting principles. Transactions are mathematically correct, appropriately summarized, and recorded in the entity's books and records.
- *Presentation and Disclosure* – Items in the financial statements are properly described, sorted, and classified.

Considers Materiality – Reflects the concept of materiality in fair financial statement presentation.

Approaches to Applying the Principle

Identifying Financial Statement Assertions

To identify relevant financial statement assertions, management starts with the financial statements, including disclosures, and identifies significant financial statement accounts, based on management's estimate of materiality. For each account and disclosure management then identifies relevant assertions, underlying transactions and events, and processes supporting these financial statement accounts.

Complies with GAAP
Supports Informative Disclosures
Reflects Company Activities
Are Supported by Relevant Financial Statement Assertions
Considers Materiality

Considering the Range of Assessment Activities

Management, with audit committee review, considers the range of the company's activities to assess whether all are appropriately captured in the financial statements, and considers whether the financial statements appropriately communicate to readers economic reality in a useful form.

Complies with GAAP
Supports Informative Disclosures
Reflects Company Activities
Are Supported by Relevant Financial Statement Assertions
Considers Materiality

Comparing Accounting Policies

Management compares the accounting principles adopted for the company to those used by companies of similar size and industry. Management also compares the content and level of detail in the company's financial statements to those organizations' reports. Significant variations are considered by management and summarized for board review.

Complies with GAAP
Supports Informative Disclosures
Reflects Company Activities
Are Supported by Relevant Financial Statement Assertions
Considers Materiality

Examples of Applying the Principle

Reviewing Financial Accounting Polices

Management of a $100 million test preparation company reviews its accounting principles by considering:

- The appropriateness of its financial reporting policies, focusing on their relevance and support of quality of reporting.
- Incentives that motivate managers to adopt one accounting policy over another.
- Relationship to controversial accounting policies used in the industry.
- Differences in its accounting policies from those of its peers.

Complies with GAAP
Supports Informative Disclosures
Reflects Company Activities
Are Supported by Relevant Financial Statement Assertions
Considers Materiality

Considering Financial Reporting Processes

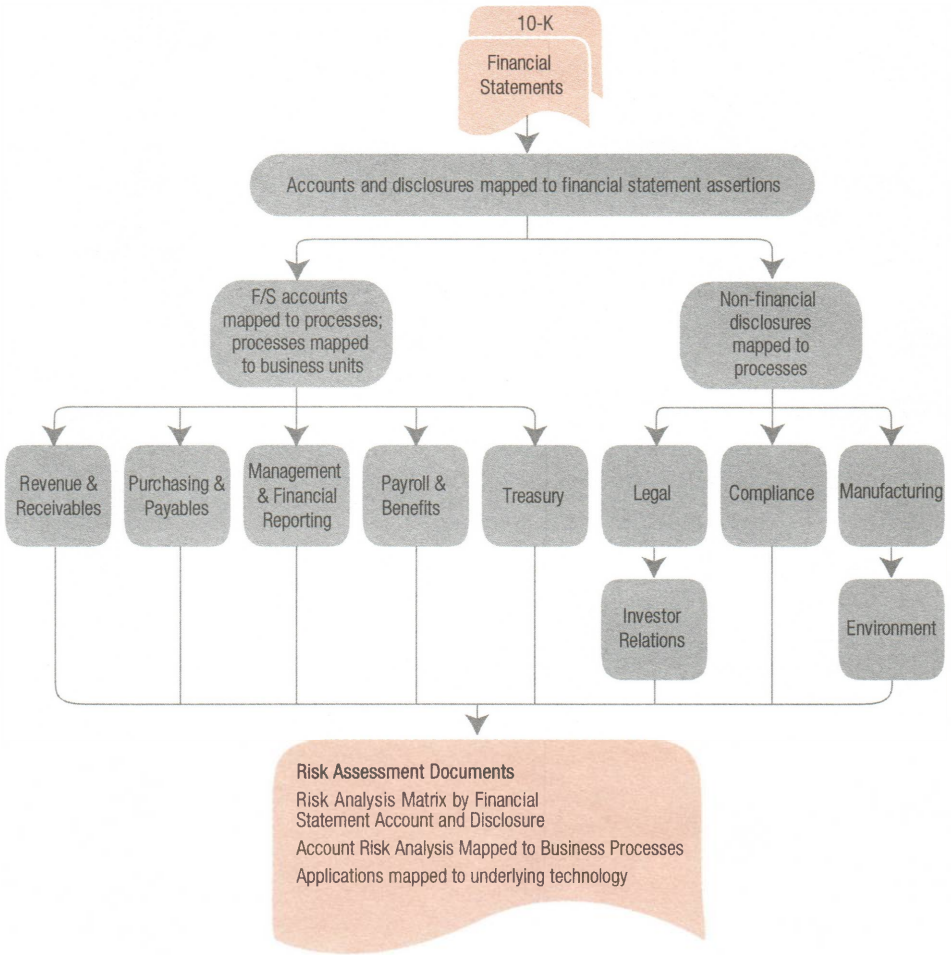
A supplier of in-home purified water and water coolers reviewed its sales process to determine which subsystems support the related account balances. Management categorized sub-processes as those that directly impact financial reporting versus those that primarily contribute to profitability of the company's operations. Management determined that sub-processes for shipment of product, invoicing, and cash collection fall into the former category, with those for credit checking and customer service falling into the latter. While reviewing the latter sub-processes might identify opportunities to reduce credit losses or loss of customers, management decided those sub-processes are not sufficiently relevant to financial reporting to include in its financial reporting objectives. The limited potential impact of the credit checking sub-process on the allowance for bad debts is compensated for by detailed analysis of accounts receivable at period end.

Complies with GAAP
Supports Informative Disclosures
Reflects Company Activities
Are Supported by Relevant Financial Statement Assertions
Considers Materiality

Complies with GAAP
Supports Informative Disclosures
Reflects Company Activities
Are Supported by Relevant Financial Statement Assertions
Considers Materiality

Linking Accounts, Assertions, and Risks

Management of a 900-person manufacturer of heavy duty transmission equipment begins its risk assessment process after establishing financial reporting assertions relevant to its financial statement accounts and disclosures. Management reviews the company's activities and interim reports in setting a level of materiality and determining whether all significant matters have been captured. This information is used as a guideline in focusing on detailed risks within each financial statement line item and disclosure supported by a series of assertions and risks to their achievement identified and carefully assessed. This approach is diagrammed below.



Principle 9
Financial Reporting Risks

The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.

Attributes of the Principle

Includes Business Processes – Risk identification includes consideration of the business processes that impact financial statement accounts and disclosures.

Includes Personnel – Risk identification and assessment considers the competency of company personnel supporting the financial reporting objectives.

Includes Information Technology – Information technology infrastructure and processes supporting the financial reporting objectives are included in the financial reporting risk assessment.

Involves Appropriate Levels of Management – The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.

Considers Both Internal and External Factors – Risk identification considers both internal and external factors and their impact on the achievement of financial reporting objectives.

Estimates Likelihood and Impact – Identified risks are analyzed through a process that includes estimating the likelihood of its occurrence and potential impact of the risk.

Triggers Reassessment – Management establishes triggers for reassessing risks as changes occur that may impact financial reporting objectives.

Approaches to Applying the Principle

Applying a Risk Identification Process

Management's risk identification process includes identifying:

- Relevant financial statement assertions for each significant account and disclosure.
- Business processes and business units supporting financial statement accounts and disclosures.
- Information technology (IT) systems supporting key business processes relevant to financial reporting objectives.

Mapping Controls

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Management maps its controls to the five internal control components in flow charts, with headers that list the activity's control objectives and risks. This approach targets activities that might generate accounting errors.

Interacting with External Parties

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

As part of a company's risk identification, management interacts with external parties that may affect the reliability of financial reporting, including suppliers, investors, creditors, shareholders, employees, customers, intermediaries, and industry peers.

Considering External Factors

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Management considers external factors that impact its ability to achieve its financial reporting objectives, such as economic, competitive, and industry conditions; regulatory and political environment; and changes in technology, supply sources, customer demands, or creditor requirements. Management also considers how internal factors and changes in them impact the company's ability to achieve its financial reporting objectives. These include account characteristics, business process characteristics, and entity-wide factors.

Updating Risk Assessments

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Management updates risk assessments on a quarterly basis, considering:

- Newly identified risks determined to be significant.
- Escalation of previously identified risks to higher relevance.
- The status of action plans to mitigate significant risks.

This risk assessment evaluates risk based on potential impact and likelihood of risks. The resulting assessment is used as a key input in determining required control activities.

Meeting with Company Personnel

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Key finance personnel meet on a regular basis with:

- Executive management to identify new initiatives, commitments, and activities affecting risks to financial reporting.
- Information technology personnel to monitor changes in information technology that may affect risks related to financial reporting.
- Human resources staff to identify and assess how changes in the workforce may affect competencies needed for internal control over financial reporting.
- Legal counsel to stay abreast of legal/regulatory changes.

Examples of Applying the Principle

Analyzing Risk Across Functions

A $120 million firearms manufacturer's CFO convenes department heads of marketing, production, information technology, human resources and administration and performs a risk analysis by functional department. Risks are rated from 1 to 5 (1 involving the least risk and 5 the most) based on potential impact on financial reporting and likelihood of occurrence. The analysis is performed by discussion in a working session format, with results documented in a table that outlines each specific risk together with the rating and factors contributing to the rating. For example, risks related to revenue recognition include:

- Revenue might not be recognized in accordance with GAAP
- Risk rating = 5
- Factors contributing to risk rating:
  - Complexity of rules for revenue recognition
  - Knowledge level of people responsible for recording sales transactions
  - Complexity of promotion and discount transactions
  - Aggressive sales targets
  - Incentive and bonus structure
  - Supporting systems limitations

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Analyzing Risks in Third-Party Operations

In analyzing its payroll and employee benefits, a metals distributor identifies risks related to completeness and accuracy of employee data maintained by its third-party service provider. Identified risks include risks related to ineffective data entry procedures which could lead to incomplete or inaccurate processing of data by the payroll administrator, and risks related to the fraudulent setup of fictitious employees, potentially leading to misstated financial reports.

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Analyzing Risk for Information Technology

In a spirits distillation and distribution company with three information technology support personnel, risk assessment is driven by the number and complexity of applications that support the financial reporting process. This approach helps the company establish on which information systems management relies for financial reporting. Prior to implementation of new systems and when significant changes to existing systems are planned, the company takes the following steps:

1. IT managers meet with the business process owners to consider IT-process related risks. The managers gain an understanding of how application data are used in the financial reporting process, identify risks of inaccurate or incomplete processing, and consider existing general computer controls in determining whether computer application controls or related user controls need to be enhanced.
2. IT managers map the related applications to the operating systems, databases, and supporting IT processes, and consider inherent risks and what improvements are needed.
3. IT managers review opportunities to automate manual controls to improve efficiency.

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Setting Triggers to Reassess Financial Reporting Risks

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Management of a technology component manufacturing company established a set of criteria that trigger a need to reassess financial reporting risks. The criteria center on risks related to new regulatory reporting requirements, changes in industry practices and significant changes within the company, including:

- Significant information technology related changes within the company (e.g. major system conversion/module conversion)
- Financial performance variances around revenue, gross margin and/or cost parameters
- Key functional leadership changes (e.g. loss of leader/director of research and development, production, product management quality control)
- Significant changes in accounting standards
- Merger, acquisition, use of derivatives or other action involving complex accounting requirements

Should any of these changes become likely to occur, functional leadership is required to develop "what if" scenarios and a risk mitigation action plan.

Assessing Risks to Significant Financial Statement Accounts

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Management of a wholesale marine supply company identifies risks to achievement of financial reporting objectives by considering risk factors related to each significant financial statement account and disclosure item. The risk identification and analysis process considers both quantitative and qualitative factors, including the risk of fraud, analyzing the following factors:

- *Impact on Financial Statements* – A quantitative measure is used to measure potential impact on financial reporting objectives. Each account is assessed in relation to its respective category, such as total assets or revenues. Accounts less than 5% are deemed low risk, those 5% or greater but less than 10% are considered medium risk, and those 10% or greater high risk. Where risks vary by sub-account, management considers risk at that level, and management also considers the potential for certain accounts being understated.
- *Account Characteristics* – Management considers internal factors such as volume of transactions through an account, judgment required, and complexity of accounting principles. Management also considers such external factors as economic, competitive, and industry conditions, regulatory and political environment, new rules/regulations affecting the account, and changes in technology, supply sources, customer demands, or creditor requirements.
- *Business Process Characteristics* – Management identifies business processes that generate transactions in each of the financial statement accounts, considering factors such as complexity of the process, centralization versus decentralization, IT systems supporting the process, changes made or new processes added, and interaction with external parties such as with vendors, creditors, shareholders, or customers.
- *Fraud Risk* – For susceptible accounts, management assesses the risk of misstatements due to fraud.
- *Entity-Wide Factors* – Management considers such internal entity-wide factors as nature of the company's activities, employees' access to assets, number and quality of personnel

and levels of training provided, changes in information systems, and such organizational changes as changes in key personnel or responsibilities. These factors are considered in relation to their effect on account characteristics, business process characteristics, and fraud risk.

Using Risk Ratings

Management of a health care organization developed a rating system providing a directional measure of relative risks, and uses the ratings to determine which processes require more in-depth attention. Relevance of the financial reporting assertions for the related accounts also is considered. The ratings are as follows:

- *High* – Critical processes that require more in-depth documentation, including a risk/controls matrix to describe key risks and controls that mitigate the risks. Process maps and narratives also are developed to describe the flow of transactions and to identify control points. Controls are identified as preventive or detective, and manual or computer-based. Policies and procedures that guide employees in applying control activities are identified.
- *Medium* – Processes for which management prepares process documentation that includes a risk/controls matrix to describe key risks and controls that mitigate the risks. Process maps and narratives are developed where applicable at a high level. Policies and procedures are identified, but in less formal summary form.
- *Low* – Processes that require minimal process documentation, which may address only key policy/procedures and applicable controls.

This risk assessment information is updated periodically. Information technology managers meet with finance personnel monthly to discuss process/changes/projects in each functional area relating to financial reporting. The meetings are used to update team members and discuss issues or changes to the processes. Additionally, management meets with outside legal counsel quarterly to discuss effects of any external regulatory changes that may impact financial reporting.

Includes Business Processes
Includes Personnel
Includes Information Technology
Involves Appropriate Levels of Management
Considers Both Internal and External Factors
Estimates Likelihood and Impact
Triggers Reassessment

Principle 10
Fraud Risk

The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

Attributes of the Principle

Considers Incentives and Pressures – Management's assessment of fraud risks considers incentives and pressures, attitudes, and rationalizations, as well as opportunity to commit fraud.

Considers Risk Factors – A company's assessment considers risk factors that influence the likelihood of someone committing a fraud and the impact of a fraud on financial reporting.

Establishes Responsibility and Accountability – Responsibility and accountability for fraud policies and procedures reside with management of the business unit or process in which the risk resides.

Approaches to Applying the Principle

Reviewing Incentives and Pressures Related to Compensation Programs

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

The board and management review the company's compensation programs and company's performance evaluation process to identify potential incentives and pressures for employees to commit fraud. This review considers how meeting, or not meeting, financial reporting targets potentially impacts individual's evaluation, compensation, and continued employment.

Conducting Fraud Risk Assessments

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

Management conducts a comprehensive fraud risk assessment to identify the various ways that fraud and misconduct can occur, considering:

- Fraud schemes and scenarios that are common to the industry sectors and markets in which the company operates
- Geographic regions where the company does business
- Unusual, or complex transactions subject to significant management influence
- Nature of automation
- Degree of estimates and judgments in financial reporting
- Last minute transactions
- Vulnerability to management override and potential schemes to circumvent existing control activities.

From these considerations, management makes an informed assessment of specific areas where fraud might exist and the likelihood of their occurrence and potential impact.

Considering Approaches to Circumvent or Override Controls

In identifying, evaluating, and testing the design and operating effectiveness of entity-wide controls that address fraud, management considers how individuals might seek to circumvent or override controls intended to prevent or detect fraud.

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

Using Information Technology Tools

Management uses, where practical, information technology tools including security systems, fraud detection and monitoring tools, and incident tracking systems to identify and manage fraud risk.

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

Developing Incident Investigation and Remediation Processes

Management develops a structured process for incident investigation and remediation. Investigation roles and responsibilities are clearly delineated, and the processes include a tracking mechanism that allows management to report on material fraud events.

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

Internal Audit Considering Fraud Risk

The person responsible for the internal audit function incorporates results of the fraud risk assessment into the internal audit plan. Management reviews and confirms that the internal audit plan addresses relevant risks.

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

Examples of Applying the Principle

Detecting Fictitious or Misreported Sales

A car dealership with three locations compensates employees based on the number of vehicles sold each month. The highest performing sales persons are awarded a bonus. Any salesperson with the fewest sales for two consecutive months is terminated. This arrangement resulted in employees creating fictitious sales and reporting sales in a later period. To mitigate this risk:

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

- The general manager reviews all sales recorded in the first and last five days of each month for indication of inappropriate reporting
- Each sales person is required annually to sign a statement whether they understand the policy and have appropriately entered sales into the system
- The company contracts with an auditor, among other procedures, to review selected sales entries.

Management is positioned to better assess accurate and timely reporting, in some instances resulting in recasting bonuses and in one case termination of a salesperson.

Preventing Bribery in the Shipbuilding Industry

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

A 750-person shipbuilding company engages in repair, conversion, and construction of military and commercial ships. To help assess compliance with applicable anti-bribery laws, the company's ethics policy has strict and clear language on what constitutes bribery, what is allowed or not regarding giving and receiving of gifts and personal relationships with government and other customers. The company maintains an anonymous ethics hotline and encourages employees to report any potential breaches of the ethics policy by co-workers, with reports of suspected impropriety immediately reported to senior management. All employees are required to sign off on adherence to the company's ethics policy upon hire and annually.

Preventing Gift Card Fraud in the Retail Sector

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

Management of a chain of menswear stores specializing in tailored clothing, accessories, and sportswear offers gift cards to its customers. The company identified instances where a store clerk provided paying customers gift cards containing no value and pocketing the real card. To combat this fraud, management implemented a policy whereby store clerks enter all gift card transactions into the register and the store manager signs off electronically on the transactions. Evidence of this sign-off is retained by the store manager and submitted monthly to the CFO.

Reporting and Investigating Fraud at a Consumer Finance Company

Considers Incentives and Pressures
Considers Risk Factors
Establishes Responsibility and Accountability

Management of a 160-employee consumer finance company established a standardized process for reporting and investigating suspected fraud. The company has a whistle-blower hotline through which employees report potential instances of fraud. After initial screening by the external vendor which manages the hotline, a three-person team to conducts an investigation, with oversight by the Controller. The Controller manages the status of the investigation through a centralized case management system, which generates periodic status reports provided quarterly to top management and the Audit Committee.

III. Control Activities

Control activities are performed at various levels of a company to reduce risks to achievement of financial reporting objectives.

At a high, entity-wide, level management compares actual performance to budget and forecast, reviews financial reports, and considers operational and financial performance indicators. Wide spans of control allow management of smaller businesses to use these types of reports effectively to manage the business and to detect deficiencies in the operation of process-level control activities and changes in operations that may warrant attention. Some activities performed by managers serve as both a control activity and a monitoring activity, and users may wish to consider the guidance on monitoring in Chapter 6 when evaluating the effectiveness of control activities.

At other levels throughout an organization procedures in business processes capture and record information in the company's accounts. Control activities in smaller companies often rely on communication channels where senior managers communicate directly with other employees. Management establishes information technology controls as needed to support financial reporting objectives. Where resource constraints compromise the ability to segregate duties, many smaller companies use certain compensating controls to achieve the objectives.

Four principles relate to control activities:

11. **Integration with Risk Assessment** – Actions are taken to address risks to the achievement of financial reporting objectives.
12. **Selection and Development of Control Activities** – Control activities are selected and developed considering their cost and potential effectiveness in mitigating risks to the achievement of financial reporting objectives.
13. **Policies and Procedures** – Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.
14. **Information Technology** – Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Guidance useful in implementing or assessing the application of the principles is provided in the balance of this chapter, with additional illustrative guidance included in Volume III.

Principle 11
Integration with Risk Assessment

Actions are taken to address risks to the achievement of financial reporting objectives.

Attributes of the Principle

Mitigates Risks – Control activities respond to risks, mitigating their potential impact on financial reporting objectives.

Considers All Significant Points of Entry into the Company's General Ledger – Control activities consider risks related to all aspects of the recording process, including accounting estimates and adjusting and closing journal entries.

Considers Information Technology – The selection of control activities encompasses relevant information technology risks.

Approaches to Applying the Principle

Considering Entity-Wide Controls

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Management considers entity-wide controls that are pervasive across the company when considering whether control activities are sufficient to address identified risks. Management then makes informed decisions as to which processes need additional detailed controls. Control activities (both entity-wide and controls over detailed processes) consider risks inherent in processing relevant classes of transactions where errors or fraud could occur, individually or in the aggregate, such as to adversely affect achievement of financial reporting objectives.

Using Workshops to Identify and Evaluate Controls

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Management uses workshops to identify appropriate control activities for each identified risk to a financial reporting objective and to train its employees in proper implementation of control activities.

Using Matrices to Identify and Evaluate Controls

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Management uses risk/control matrices developed in the process of assessing risks and designing controls in each business process to perform a "gap analysis" to evaluate the need for any additional controls that might be needed to mitigate risks to the achievement of financial reporting objectives.

Using an Inventory of Controls to Identify and Evaluate Controls

Management uses software that provides an inventory of controls typically aligned to specified risks to financial reporting. Use of the pre-populated inventory of common controls by business process facilitates identification, implementation, and testing of relevant control activities.

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Using SAS 70 Reports

When outsourcing all or a portion of its financial reporting function, the CFO obtains a SAS 70 Type II report or undertakes procedures to assess controls in place for the initiation, recording, and processing of significant classes of transactions at the third-party outsourcer.

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Examples of Applying the Principle

Focusing on Accounting Estimates and Adjusting Entry Risks and Controls

A $220 million manufacturer of sporting goods equipment in conjunction with its risk assessment process develops a spreadsheet setting out the financial reporting objectives and relevant assertions, identified risks, and control activities. This effort considers matters such as general ledger maintenance, accruals, management estimates and reserves, period-close and consolidation procedures, financial statement preparation, and regulatory filings and disclosures. Management reviews the type of control activity (preventive versus detective, manual versus automated, error versus fraud) in considering the adequacy of the control activities in reducing risks to reliable financial reporting to an appropriate level. The risks and controls are described in sufficient detail to allow management and others to evaluate effectiveness.

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Using Templates of Common Control Activities

A healthcare products and services provider with market capitalization of $70 million uses a template of common risks and control activities relating to human resource activities. Management reviews the list of common control activities and links them to risks identified in its risk assessment to develop policies and procedures appropriate to its business. Management uses the template also to identify any potential risks not previously noted, and implements additional control activities considered necessary.

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Using a SAS 70 Report from a Service Payroll Provider

A 250-person company that packages and distributes organic produce uses a third-party service organization to process payroll. The service organization engages a service auditor to audit its controls over transaction initiation, processing, and recording, and to issue a SAS 70 Type II report. The company obtains the report and considers whether the described control objectives, procedures, and test results are adequate for its needs. Because the report covers only a six-month period, and does not cover the last 3-month period of the company's fiscal year, management communicates directly with the service organization, inquiring of any changes to its processes and obtaining relevant information. Depending on the results, the company expands its review of payroll related information for the three-month period, or with the service organization's concurrence engages the service auditor to expand the scope of its audit.

Mitigates Risks
Considers All Significant Points of Entry into the Company's General Ledger
Considers Information Technology

Principle 12
Selection and Development of Control Activities

Control activities are selected and developed considering their cost and potential effectiveness in mitigating risks to the achievement of financial reporting objectives.

Attributes of the Principle

Considers Ranges of Activities – Control activities include a range of activities that vary in terms of cost and effectiveness, depending on the circumstances. These include approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

Includes Preventive and Detective Controls – Management uses an appropriate balance of preventive and detective controls, and an appropriate balance of manual and automated controls, to mitigate risks to the achievement of financial reporting objectives.

Segregates Duties – Duties are logically divided among people or processes to mitigate risks and meet financial reporting objectives.

Considers Cost vs. Benefit – When selecting among alternative control options, management considers the cost of control activities in relation to expected benefits of improved control.

Approaches to Applying the Principle

Separating Incompatible Activities

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Management separates incompatible activities by assigning them to different personnel or through implementation of information technology applications. Information technology, for example, is used to restrict access to data and programs, thereby enhancing segregation of duties, or to detect all unauthorized access to data or programs.

Monitoring When Restricting Access Is not Practical

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Where limiting access to accounting records is not practical, management, process owners, or internal auditors monitor the records closely for potential misstatements.

Providing a SAS 70 Report

Management outsources some of its operations to a third party, which is contractually obligated to report to the company on relevant controls, and provides a SAS 70 report from its auditors.

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Assessing the Cost vs Benefit of Various Control Approaches

Management assesses the costs of addressing identified risks using various control approaches, and weighs the costs against effectiveness of the controls in mitigating the respective risks. Management focuses on designing a mix of manual and/or information technology-based controls that are preventive or detective, as appropriate, and considers the relative cost effectiveness of these controls. Management also confirms that the controls, taken together, provide reasonable assurance that risks to the achievement of financial reporting objectives relating to each process are appropriately mitigated.

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Using Organizational Charts to Identify Incompatible Functions

Using organization charts, process flowcharts or other means by which activities are documented, management identifies any incompatibilities in functions and maintains appropriate segregation of duties. The documentation is regularly updated to reflect current responsibilities and activities.

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Considering Compensating Controls

Where resource constraints compromise the ability to segregate duties to achieve financial reporting objectives effectively, management considers compensating control activities, such as periodic management reviews of reports prepared in sufficient detail and in a timely fashion to enable identification of misstatements.

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Examples of Applying the Principle

Using Preventive and Detective Controls to Safeguard Assets

A precious metals mining company maintains significant quantities of gold in its warehouse. The company designed three levels of defense against unauthorized access to the gold inventory. First, as a preventive control, the gold is stored in a vault with dual locks and only the mill manager and production manager each having one of the combinations. Second, also as a preventive control, the vault is secured in a separate room used only to pour and store the gold, with access to the room restricted to the mine manager, production manager, mill manager, and mine security. Third, as a detective control, all gold added to or removed from the vault is weighed and logged, with the log under the control of the mine manager. Further, the gold is weighed and reconciled to the log by an internal auditor on a weekly basis, at the end of each financial reporting period, and before shipment of gold from the mine.

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Segregating Cash Payments

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

An operator of retail restaurants and bakeries with only a few office employees considered how best to segregate cash payments from the record-keeping process. Management decided that all checks require the signatures of both the CEO and CFO. The person preparing the checks and recording disbursements neither opens the bank statement nor performs the bank reconciliation, which procedures are performed by another individual. Another company with a similar challenge implemented software that prints electronic signatures on checks. The CEO and CFO of that company are required to review and approve disbursements pending in the system before the checks are produced.

Segregating Access to Inventory

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

An integrated multi-channel provider of modern design furnishings and accessories stores in a locked storeroom materials and supplies used in constructing, repairing, and refinishing furnishings. The company lacks segregation between storeroom access and related accounting records, resulting in risk that inventory could be lost or misappropriated without detection. As compensating controls materials and supplies are spot-checked periodically and reconciled by the purchasing manager with the accounting records, and the capability to enter transactions or modify related account balances is limited to individuals without storeroom access. These compensating controls provide management reasonable assurance that recorded inventory balances are accurate.

Segregating Access to Purchases

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

A $100 million designer, manufacturer, and distributor of consumer and industrial optical products has two staff in its purchasing department, with both authorized to prepare purchase orders up to $5,000. Because purchase orders are not reviewed prior to being sent to vendors, a risk exists that unintentional errors or intentional acts will result in inventory valuation errors, obsolescence, or shortages due to diverted shipments. To reduce risk to an acceptable level, management relies on a combination of actions of other staff, including the:

- *Inventory receiving clerk*, who evaluates, documents, and reports to management unusual inventory movement such as excessive ordering that could lead to obsolescence
- *Inventory clerk*, who documents and tracks all inventory levels, reducing the risk of obsolescence.
- *Payables clerk*, who matches payable invoices to purchase orders and receiving reports before amounts are paid, reducing the risk of errors resulting from diverted shipments.
- *Controller*, who reviews exception reports of all inventory purchases with a price more than 15% above current average costing.

Taken together, these controls result in management assessing risk as acceptable.

Segregating Access to Fixed Assets

A 340-employee provider of information storage equipment maintains fixed assets in the form of computer and network equipment. There are significant numbers of fixed asset acquisitions, retirements, and disposals, with transactions recorded by a staff accountant. The accountant records the transactions in a spreadsheet-based property ledger, posts the related entries to the general ledger, and monthly reconciles the two ledgers. To address risk resulting from a lack of segregation of duties – which risk relates to theft of fixed assets and error or fraud in accuracy or completeness of processing – the controller spot checks the entries and reviews the monthly reconciliations. The controller also includes a budget-to-actual analysis of capital expenditures and summary of fixed asset changes in monthly reports provided to senior operating managers who are positioned to question information at odds with their knowledge of business activities. These compensating controls reduce the associated risks to a sufficiently low level.

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Balancing Cost and Effectiveness

A provider of marine transportation equipment to the oil and petroleum industries maintains a significant amount of inventory on hand at the end of any quarter. The company has a simple accounting system in place that tracks inventory purchases and allocates costs to finished goods as each new piece of equipment is completed. As part of the company's risk assessment process, management reviews the risks within the inventory process and the potential impact on reliability of financial reporting. To address mitigating the risk that recorded inventory quantities do not reflect amounts on hand, management considered a rigorous process of extensive quarterly inventory counts, or as an alternative, performing periodic cycle counts. Management concluded that periodic cycle counts would reduce risk to an acceptable level.

Considers Ranges of Activities
Includes Preventive and Detective Controls
Segregates Duties
Considers Cost vs. Benefit

Principle 13
Policies and Procedures

Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.

Attributes of the Principle

Integrates into Business Processes – Control activities are built into business processes and employees' day-to-day activities.

Establishes Responsibility and Accountability – Responsibility and accountability for policies and procedures resides with management of the business unit or function in which the relevant risk resides.

Occurs on a Timely Basis – Procedures are performed in a timely manner.

Thoughtfully Implements – Procedures are implemented thoughtfully, conscientiously, and consistently across the business. Procedures reflect policies developed at the senior management level as well as those with more specificity developed at the function, department, and process levels.

Investigates Exceptions – Conditions identified as a result of executing the procedures are investigated and appropriate actions are taken.

Periodically Reassesses – Policies and procedures are reviewed periodically to determine their continued relevance.

Approaches to Applying the Principle

Developing and Documenting Policies and Procedures

Integrates into Business Processes
Establishes Responsibility and Accountability
Occurs on a Timely Basis
Thoughtfully Implements
Investigates Exceptions
Periodically Reassesses

Management develops and documents policies and procedures for all significant financial reporting related activities using various formats such as narratives, flowcharts, and control matrices. Management develops a standardized format for its policies, which includes:

- Reason for or purpose of the policy
- Locations/units/processes to which the policy applies
- Roles and responsibilities for ownership, creation, implementation, execution, and maintenance of the policy
- Matters covered by the policy
- Escalation procedures for policy exceptions
- Review date

Considering Preventative and Detective Controls

Management includes both preventative and detective controls within each process, using process maps, narratives, spreadsheets, or other mechanisms to document and communicate the control activities.

Integrates into Business Processes
Establishes Responsibility and Accountability
Occurs on a Timely Basis
Thoughtfully Implements
Investigates Exceptions
Periodically Reassesses

Developing Policies for Entity-Wide Applications

Central management develops policies for areas that have entity-wide application, such as its code of conduct, delegation of authority, safeguarding of assets, and so forth. In addition, management develops policies at the business unit level that support and align with entity-wide policies.

Integrates into Business Processes
Establishes Responsibility and Accountability
Occurs on a Timely Basis
Thoughtfully Implements
Investigates Exceptions
Periodically Reassesses

Examples of Applying the Principle

Using Templates to Document Policies

A natural gas utility uses a standardized template to format its policies. Its credit and collection policy addresses:

Integrates into Business Processes
Establishes Responsibility and Accountability
Occurs on a Timely Basis
Thoughtfully Implement
Investigates Exceptions
Periodically Reassesses

- *Purpose* – outlines the required credit application and approval process used to extend trade credit to customers.
- *Location* – specifies the policy's geographic boundaries that it applies company-wide across all regions and business units.
- *Key Provisions* – covers steps from credit application initiation through credit checks and approval for credit and credit limit.
- *Roles and Responsibilities* – describes the roles/responsibilities of all those involved in the credit application and approval process including the timeframe for completion. This includes the sales representative (submits the credit application), credit analyst (performs credit check and recommends credit limit), controller (reviews the credit check and approves credit limit), and customer service manager (enters the credit limit into the customer file). Where these responsibilities are carried out by the same person, the lead manager of the business unit or function is required to consider how such responsibilities should be segregated or compensating controls established.
- *Escalation Procedure for Exceptions* – specifies that requests for exceptions to the credit policy must be elevated to the controller, CFO, CEO or the board, depending on specified monetary thresholds.
- *Review Date* – specifies when the policy should be reviewed, with policies related to high-risk accounts required to be reviewed more frequently than those for lower-risk accounts.

Documenting and Approving Policies

A business-to-business media company formally documents policies for its key business processes in the form of policy statements, which are approved by the board and communicated to employees through the company intranet. The policy statements deal with spending authority, revenue recognition, expenditure requisitions, code of conduct, whistle-blower process, and fixed asset acquisitions, depreciation, and disposition. For other processes whose risks are deemed non-critical but still important (as assessed during the risk analysis process) – including invoicing, distribution, and collections – procedures and controls are approved by management and documented in the risk/controls matrix.

Integrates into Business Processes
Establishes Responsibility and Accountability
Occurs on a Timely Basis
Thoughtfully Implements
Investigates Exceptions
Periodically Reassesses

Policies for Cash Disbursements

Integrates into Business Processes
Establishes Responsibility and Accountability
Occurs on a Timely Basis
Thoughtfully Implements
Investigates Exceptions
Periodically Reassesses

A distributor of personal care and nutritional supplement products establishes a policy that all payments must be appropriately authorized before cash is remitted. The policy applies at all company levels, with approval limits set in relation to authority of the individual or group. The policy establishes that transactions involving smaller cash payments – up to $500 – may be approved by a payables clerk, but higher amounts must be approved as follows: up to $2,500 by the controller, $20,000 by the CFO, $100,000 by the CEO, and over $100,000 by the board.

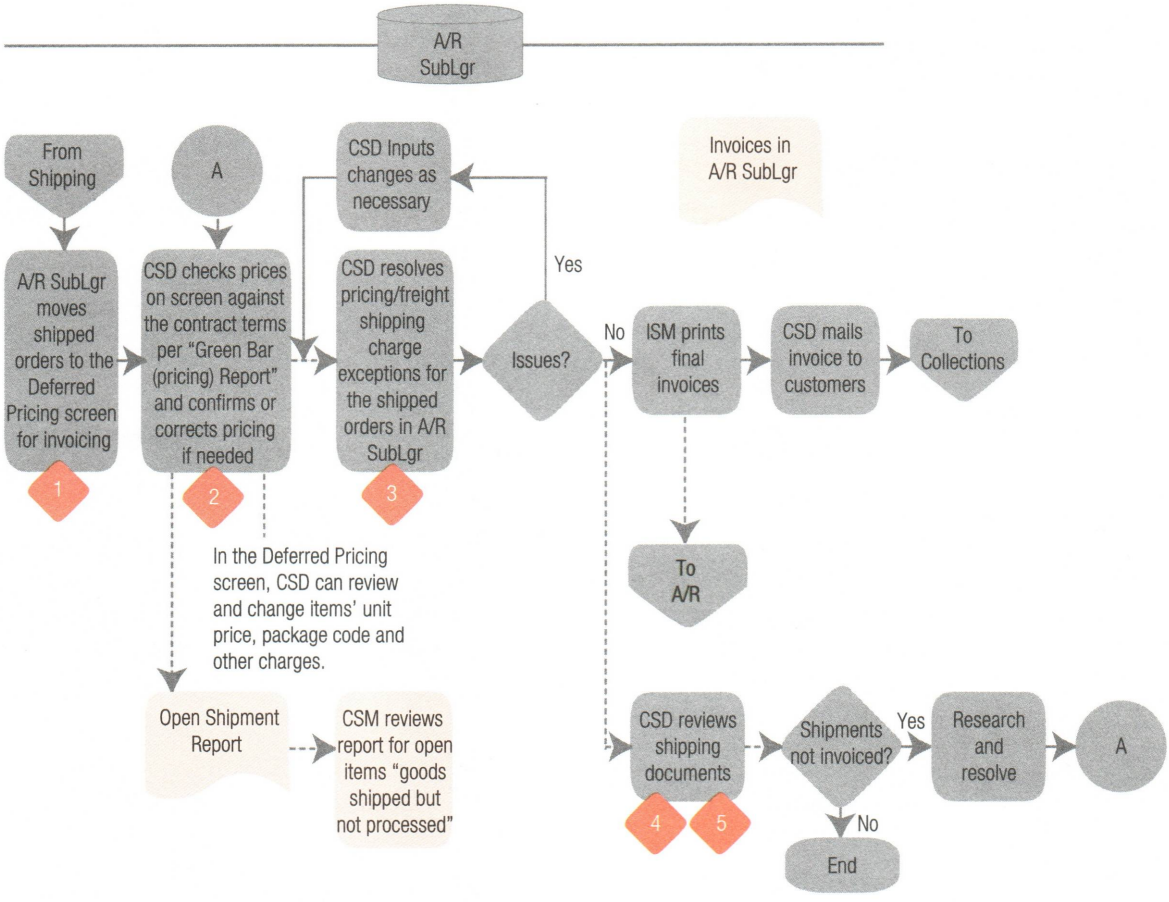
Using Software to Document Control Activities

Integrates into Business Processes
Establishes Responsibility and Accountability
Occurs on a Timely Basis
Thoughtfully Implements
Investigates Exceptions
Periodically Reassesses

An international order processing company flowcharts its control activities using "off the shelf" software. The flowchart and accompanying narrative provide the following benefits:

- The nature of the control procedures is clearly documented in context of business processes.
- Responsibilities for performing control procedures are set forth, enhancing communication.
- The documentation of the controls provides a basis for testing their effectiveness.

Presented on facing page is a flowchart illustrating part of the company's revenue cycle.

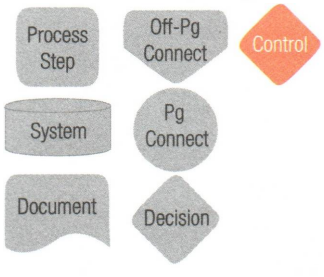


CONTROLS

1. After shipment, automated controls move the order to deferred pricing status to facilitate final review. Order will not invoice until review is complete.
2. Before invoicing, CSD confirms contract terms and pricing by comparing prices on screen to Pricing Report.
3. Before issuing invoice, CSD confirms pricing & delivery terms (Freight, Surcharges, etc.) by reconciling draft invoice to A/R Sub-ledger Pricing Report.
4. At month-end, CSD reviews deferred pricing screen and ensures that all shipments have been invoiced. The CSM reviews the Open Shipments Report to ensure all shipments are invoiced or accrued.
5. At month-end, CSD reviews shipping records and terms per individual contracts to ensure that title has transferred for all shipments invoiced and booked as sales.

LEGEND

CSD Customer Service Department
ISM Information Systems Manager
CSM Customer Service Manager



Principle 14
Information Technology

Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Attributes of the Principle

Includes Application Controls – Application controls are:

- Built into computer programs and supported by manual procedures.
- Designed to provide completeness and accuracy of information processing critical to integrity of the financial reporting process.

Considers General Computer Operations – General computer controls are broad and include controls over access, change and incident management, systems development and deployment, computer operations, data backup and recovery, third party vendor management, and logical and physical security critical to the integrity of the financial reporting process.

Includes End-User Computing – End-user computing processes, including spreadsheets and other user-developed programs, are documented, secured, backed up, and regularly reviewed for processing integrity.

The extent of the needed information technology controls is derived from management's identification and assessment of processes and systems supporting financial reporting. These information technology systems typically are identified as part of the risk assessment process, as illustrated in the Risk Assessment chapter. Once the extent of the relevant information technology systems is determined, management may consider the complexity of those systems.

Complexity

The nature of information technology related controls is largely a reflection of the degree of complexity of transaction processing, software development and related factors:

	Less Complex	More Complex
Transaction Processing	Processing is such that input controls can be readily reconciled to the system output. Reliability of processing is achieved via manual user controls.	Transactions are subject to calculations or other manipulations using data or formulas, sometimes with multiple subsystems, where input is not reconcilable to system output. Reliability of processing is achieved via built in application controls, together with related manual user controls and IT general controls.
System Development	Packaged accounting software with straightforward functions with few processing options, or with standard, readily configurable processing options and controls. Reliability achieved through controls over vendor selection and package implementation.	Custom developed software or packaged software modified or supplemented to meet the company's processing needs. The software may require modification as additional features are provided to users or company needs change. Reliability achieved through program development and change controls.
Connectivity	Connectivity to external networks and/or the internet is limited to email applications.	Reliance on external connectivity, including the internet, where the company transmits transactional data to and from the internet.
End-User Computing	Spreadsheets serve as an electronic information warehouse, perhaps performing straightforward calculations using simple formulas.	Spreadsheets support complex calculations, valuations and modeling tools, perhaps using macros and linking multiple supporting spreadsheets.

Illustrating Less Complex Information Technology

A shoe retailer uses a highly regarded packaged system for managing store sales and inventory. The software is fully integrated with another well regarded packaged general ledger system that manages reporting and administrative functions including payments and payroll. The company has no internally developed applications that interact with these packages, and neither the company nor its personnel have the right or ability to modify the package software.

Illustrating More Complex Information Technology

A finance company runs a number of complex systems, with some packaged software but the majority being custom, in-house developed software. These systems perform complex calculations using external databases to compute interest income, product yield, etc.

Approaches to Applying the Principle

The following categorization of IT controls may be useful in considering the design of controls or evaluating their effectiveness (the first four categories comprise IT general controls). Following the category descriptions are approaches based on aforementioned degree of complexity.

- *Systems Development* – controls over design and implementation of systems that help ensure that systems are appropriately developed, configured, approved, and migrated into production.
- *System Changes* – controls over modifications to systems – whether applications, supporting databases or operating systems – helping to ensure that changes are approved and properly tested and implemented. (In less complex environments system change and systems development procedures are often combined for ease of implementation, training and ongoing maintenance.
- *Security and Access* – controls over critical applications, supporting databases, and networks that help management ensure that access is properly authorized and data is appropriately used, maintained and reported.
- *Computer Operations* – controls over day-to-day operations that help ensure that processing errors or improprieties are identified and corrected in a timely manner.
- *Application Controls* – controls built into applications to help ensure completeness and accuracy of transaction authorization, validity and processing, as well as related manual user controls.
- *End-User Computing* – controls over spreadsheet and other user-developed applications that address potential input, logic, and interface errors.

Systems Development

Less complex environments will generally have fewer significant changes to the processing environment, and might not experience any changes for long periods. Changes might include only operating system patches and packaged application upgrades.

Applying System Developing in a Less Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Within this less complex environment management follows a process for selecting new packages which considers application controls, security features, data conversion requirements, testing, and back-out plans.

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Within this less complex environment management relies on system change procedures for updates, including migration to production status. While some IT managers implement upgrades immediately, others wait several months before installation to better assess whether any bugs in the update are worked out in the end-user community. Where major upgrades are issued, there normally is a greater need for extensive testing, in which case the upgrade is subject to a more comprehensive system change control process.

Applying System Developing in a More Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Within a more complex environment management also uses a broader range of system development policies and procedures that help ensure financial reporting related applications are designed, developed, tested, and installed in a properly controlled manner.

Change Management

Change management controls address a variety of IT matters, including software application programs, system software, database administration, network and security configurations, and job scheduling.

Applying Change Management in a Less Complex Computer Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Application, database, and job schedule changes may be limited to controls over proper installation of upgrades (other elements such as network infrastructure may not be relevant).

A patch management process may be used that includes testing prior to release of packaged software updates into production or contracts with a third party to test application and system patches. The level of detailed testing depends on the complexity and nature of a change.

Applying Change Management in a More Complex Computer Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

More complex environments typically have a wide variety of changes at the request of the business or initiated by the IT group. In these environments management:

- Develops change and incident management processes, with effective control procedures to help ensure changes are made properly. Operating systems change and vendor-issued upgrades to packaged applications are implemented subject to an effectively controlled change process.
- Where the company utilizes a network for user authentication and/or receiving data such as customer orders, appropriate controls are required to determine whether changes are done properly such that reporting objectives are achieved.

Security and Access Controls

These controls address access to relevant IT elements such as applications, system software, databases, networks, and the like.

Applying Security and Access Controls in a Less Complex Computer Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

In less complex environments, access controls are focused on access to the network and access to application software. Database technology utilized by packaged application software is maintained through the application tools and interfaces. Access controls are monitored through IT operations or a security administrator.

A security administrator, for example:

- Grants and maintains access at levels defined by management, including disabling default logon accounts
- Authenticates logon accounts
- Establishes general system access control including system default passwords, implements security patches in cooperation with IT operations, and disables unnecessary services
- Monitors and reports on security issues to IT management and information owners
- Performs re-certifications.

Applying Security and Access Controls in a More Complex Computer Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

More complex environments utilizing the network for user authentication and/or receiving data (e.g. customer orders) call for network controls. Within a more complex environment management:

- Secures access to critical applications, databases, operating systems, and networks.
- Restricts access to authorized personnel by requiring appropriate identification and authentication. Server, telephone, network and power supply equipment are kept in a secured room or cabinet.
- Receives and reviews reports on both security and processing problems and delivers to an appropriate, identified individual, with problem tracking mechanisms established.

Computer Operations

Applying Computer Operations in a Less Complex Computer Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Within a less complex environment management backs up, retains, and stores critical financial data and programs. Backup media are stored in secure locations, both on-site and off-site. Back-up media is tested periodically to assess recoverability.

Applying Security and Access Controls in a More Complex Computer Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Within a more complex environment management also establishes formal sign-off procedures to track items transferred offsite for back-up purposes.

Establishes a process to report operating issues, with regular or periodic review, by IT operations and company management. Issues are analyzed to determine corrective actions, prioritized according to the impact on the company. An escalation process accelerates urgent issues to top management for resolution.

Application Controls

Applying Application Controls in a Less Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Management implements controls over data input to determine whether transactions are authorized, and transactions are processed correctly and completely, with rejected items captured and followed-up.

Implements controls over output to help ensure matters requiring user action are properly dealt with.

Applying Application Controls in a More Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Within a more complex environment management also uses data processing controls for accuracy, completeness, and timeliness of data during either batch or real-time processing by the computer application. Controls over application programs and related computer operations are reviewed to determine that data are processed accurately through the application and that no data are added, lost, or altered during processing. A formal data exception procedure exists for error handling, where management reviews all changes to data during the remediation process.

End-User Computing

Identifying and Securing End-User Computing Applications

Identifies significant end-user applications, including spreadsheets and other user-developed programs. Critical end-user applications are stored on secured file servers. Data integrity is ensured by locking or protecting cells to prevent inadvertent or intentional changes to standing data.

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Outsourced Operations

Reviewing Outsourced Operations

Some companies choose to outsource management of their information technology. Outsourced tasks may include those related to computer operations, change management and security and access controls. Management reviews general computer controls of critical third party vendors that host and/or support critical financial applications and/or information technology support functions. These controls may be evidenced by an independent third party review and report, such as a SAS 70 Type II report.

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Examples of Applying the Principle

Included here are one or two illustrative examples for each of the six categories described above. Volume III contains additional illustrations for both less complex and more complex IT environments.

Systems Development

Managing Development and Implementation of New Software in a More Complex Environment

Management of a farm equipment manufacturing company decided to replace its inventory management system with a new system to be developed in-house. The company has one systems analyst and only two programmers on staff to develop and test the system. It lacks an automated code promotion utility for version control and migration to production. In this situation controls relevant to segregation of duties normally in place were compensated for as follows:

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

- The user manager and system analyst clearly identified the required system functionality and associated risks.
- One programmer was responsible for developing the software, with the other responsible for the testing and migration of the revised software to the production environment.
- The IT manager reviewed the design and programming and managed the entirety of the process, including:
  - Review of system design structure and coding
  - Review of test results by the user department manager as well as the IT manager.
  - Tracking code version movements within the development environment and from the development library to the test environment and then to production.
  - Rigorous review by the systems analyst, IT manager and user personnel of processing results during and post implementation.

Change Management

Managing Changes to Packaged Software in a Less Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

A 500 employee manufacturer of plastic toys uses the following change management procedures for major vendor-provided upgrade to its packaged general ledger software:

- Obtains a description of change, rationale for it, impact on the company's security environment and implications for user interfaces.
- Outlines steps for a back-out plan should the upgrade not perform as expected.
- Develops a plan to test that the edit and validation rules work properly, desired system functions operate properly and produce the desired results, undesired processing results are prevented, and existing technical capabilities continue to work properly.
- Executes the tests and documents the results.
- Maintains a change control log.
- Obtains approval from management and end users of the test results prior to release into production.

Managing Change to Custom Software in a More Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Management of a provider of material-based solutions for electronic, acoustical/thermal, and coated metal applications has decided to make significant modifications to its inventory management software. The company has only two developers on staff and needs to rely on those individuals to develop, test, and migrate the software to production. As the company does not have an automated code promotion utility to control versions and migrations to the production environment, the IT manager:

- Identifies and analyzes risk resulting from changes that will be required.
- Assigns changes to developers so that each developer works on only those changes assigned to him/her.
- Assigns to the developer not responsible for a particular change responsibility for testing the change and migration to production.
- Reviews any significant changes.
- Locks versions following user acceptance testing to prohibit further change prior to release.

The IT manager also relies on manual controls to manage the code version and migration. He therefore:

- Creates a manual log listing the version of the code copied to the development environment, along with date and time, and manually tracks the migration to test and then to production.
- Separates the review of all version control procedures prior to moving the code to production from those performed by the individual responsible for the IT functions.

Security and Access

Using Password Access in a Less Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

A $120 million developer, manufacturer, and retailer of children's educational products set its password standards for critical applications, databases, operating systems, and networks so that passwords:

- Are at least eight alphanumeric characters.
- Cannot be easily guessed.
- Are required to be changed by the owner every 90 days
- Lock out users after three consecutive failed login attempts.
- Cannot be reused before twelve intervening changes.

Reviewing Logical Security in a More Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Management of a compensation and benefits consultant with 920 employees reviews logical security controls to prevent unauthorized access to its financial reporting systems:

- *User Accounts* – There are formal user account set-up and maintenance procedures to request, establish, issue, suspend, change and delete user accounts. Users are defined as any persons attempting to access a system (e.g. employees, temporary workers, vendors, and contractors).
- *Authentication Controls* – Authentication standards establish minimum requirements for unique user IDs and passwords, and a finite number of login attempts. Unique user IDs allow management to audit accesses.
- *Privileged Accounts* – Access by system and application administrators (super-users) is limited to two employees responsible for information technology security management.
- *Application Reviews* – A process is in place to periodically review configuration settings for who has access to data related to critical applications and systems. Any violations detected are reported to management.
- *Security Reviews* – Applications and systems generate security logs, allowing user activity to be monitored and security violations reported to management.

Computer Operations

Setting Parameters for Restricting External Connectivity in a More Complex Environment

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

The information technology group of a designer, developer, and marketer of high performance computer systems configures, maintains, and monitors its firewall to:

- Limit the number of accounts that are provided to firewall administrative personnel.
- Add a "drop all" rule for packets that do not match all the rules, as well as log such information.

The administrator configures routers with the following standards:

- The enable password on the router is kept in secure encrypted form.
- The number of users who can access routers and enable access only through specific network hosts is limited.

- Limits unnecessary e-directed broadcasts, including:
  - Incoming packets at the router sourced with invalid addresses
  - TCP (Transmission Control Protocol) small services
  - UDP(User Datagram Protocol) small services
  - All source routing
  - All Web services running on routers
- Unnecessary ports on routers are disabled.
- The wireless access point's configuration is set where the SSID (Service Set Identifier) is not in broadcast mode, and passwords are changed from the default.

Outsourced Operations

Includes Application Controls
Considers General Computer Operations
Includes End-User Computing

Reviewing a Third-Party Vendor

The manager of a $211 million direct marketer of eyewear and contact lenses outsources hosting and support of its financial systems to a third-party provider. The company:

- Reviews and approves the third-party's capabilities and requires a non-disclosure agreement.
- Assigns an individual to manage the relationship.
- Considers the effectiveness of the company's user controls
- Annually reviews a third-party SAS 70 Type II report identifying any deficiencies in the third party's information technology computer controls. All client considerations noted in the report are addressed by management.

IV. Information and Communication

Information systems identify, capture, process, and distribute information supporting achievement of financial reporting objectives.

Information systems in smaller organizations are likely to be less formal than in large ones, but their role is as significant. Many smaller companies rely more on manual or stand-alone information technology applications than complex integrated applications. Effective internal communication between top management and employees may be facilitated in smaller companies, due to fewer levels and numbers of personnel and greater visibility and availability of the CEO. Internal communication can take place through the frequent meetings and day-to-day activities in which the CEO and other managers participate.

Four principles relate to the information and communication component:

15. **Financial Reporting Information** – Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.

16. **Internal Control Information** – Information needed to facilitate the functioning of other control components is identified, captured, used, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.

17. **Internal Communication** – Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.

18. **External Communication** – Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Guidance useful in implementing or assessing the application of the principles is provided in the balance of this chapter, with additional illustrative guidance included in Volume III.

Principle 15
Financial Reporting Information

Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.

Attributes of the Principle

Captures Data – Data underlying financial statements are captured (optimally, at the source) completely, accurately, timely.

Includes Financial Information – Information is identified and captured for all financial transactions and events. Information is used, among other purposes, for adjusting entries and accounting estimates, as well as to monitor the reasonableness of recorded transactions.

Uses Internal and External Sources – Information is developed using internal and external sources.

Includes Operating Information – Operating information used to develop accounting and financial information often serves as a basis for reliable financial reporting.

Maintains Quality – Information systems produce information that is timely, current, accurate, and accessible.

Approaches to Applying the Principle

Using Matrices to Detail Information Flows

Captures Data
Includes Financial Information
Uses Internal and External Sources
Includes Operating Information
Maintains Quality

Process owners maintain matrices that, for each process impacting financial reporting, detail the flow of information from the point of capture through reporting. These matrices describe the information captured and how it is used within the process, including:

- Information needed to monitor and confirm completeness, accuracy, and timeliness of input and output such as batch proofs of system-generated information.
- Information needed to monitor and confirm completeness, accuracy, and timeliness of processing, including system-generated information.

Obtaining Information from External Sources

Management obtains information from external sources, such as industry publications, trade associations and conferences to identify events affecting industry trends, suppliers, customers, competitors, and the economic climate.

Captures Data
Includes Financial Information
Uses Internal and External Sources
Includes Operating Information
Maintains Quality

Meeting with Personnel from Other Business Area

Management in charge of financial reporting meets periodically with personnel from other areas of the business – such as operations, compliance, human resources, or product development – to obtain information that may affect financial reporting.

Captures Data
Includes Financial Information
Uses Internal and External Sources
Includes Operating Information
Maintains Quality

Examples of Applying the Principle

Using Matrices to Record Information Flow

The controller of an information technology hosting service uses matrices to record information flows within processes that capture information supporting financial reporting. The matrices include information on persons or functions responsible for creating, modifying, approving, using and monitoring information in each process and sub-process. An example of a matrix is presented with Principle 16, under the heading "Using Information Maps in Accounts Payable."

Captures Data
Includes Financial Information
Uses Internal and External Sources
Includes Operating Information
Maintains Quality

Using Management Meetings to Validate and Document Key Assumptions

The CEO of a perishable food procurement and marketing company meets quarterly with the CFO and department heads to validate and document key assumptions that drive the company's reserves and accruals. Accuracy of the quarterly valuations is discussed and tracked.

Captures Data
Includes Financial Information
Uses Internal and External Sources
Includes Operating Information
Maintains Quality

Using Operating Information for Financial Reporting

A manufacturer of electrical equipment and components' staff member responsible for environmental and other regulatory compliance matters meets regularly with financial management to discuss compliance and related remediation costs to enable appropriate financial reporting of those activities.

Captures Data
Includes Financial Information
Uses Internal and External Sources
Includes Operating Information
Maintains Quality

Principle 16
Internal Control Information

Information needed to facilitate the functioning of other control components is identified, captured, used, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.

Attributes of the Principle

Captures Data – Data required to execute each control component are captured completely, accurately, and timely and in compliance with laws and regulations.

Triggers Resolution and Update – Reporting triggers prompt exception resolution, root-cause analysis, and control update, as needed.

Maintains Quality – Information systems produce information that is timely, current, accurate and accessible. The quality of system information is reviewed periodically to assess its reliability and timeliness in meeting the company's internal control objectives.

Approaches to Applying the Principle

Developing and Maintaining Information Maps

Captures Data
Triggers Resolution and Update
Maintains Quality

Process owners develop and maintain information maps – spreadsheet matrices, with captions down the left side identifying information related to a particular financial statement account, and column headings identifying individuals or function associated with the information, with the information in the matrices' boxes depicting alignment of responsibilities for the account information.

Identifying Information through Discussion

Captures Data
Triggers Resolution and Update
Maintains Quality

In assessing information needs, management identifies through discussions with various personnel information used to manage and control day-to-day operations and how this information relates to accounting and financial reporting.

Examples of Applying the Principle

Using Information Maps in Accounts Payable

Captures Data
Triggers Resolution and Update
Maintains Quality

An automotive parts manufacturer with annual revenues of $250 million captures information about its accounts payable process using information maps. Authorizations are shown to be created by the controller, authorized by the CFO, and used by accounting and accounts payable, information technology, materials management, purchasing, and receiving. Monitoring responsibility is also documented.

The information map describes the use of information used as part of internal control, as well as a basis for monitoring and testing the operation of controls. Management is able to determine key parts of a process where risks to reliable information are the highest such as at various points of update, and key points of monitoring.

	Department / Function							
Information Element	**Finance**	**Accounts Payable**	**CFO**	**Controller**	**Information Technology**	**Materials Management**	**Purchasing**	**Receiving**
Accounting								
Account description	C	U	M	M	U	U	U	U
Account code	C	U	M	M	U	U	U	U
Authorization								
Role	U	U	A	C	U	U	U	U
Name	U	U	A	C	U	U	U	U
Purchasing								
Item code	U	U	M	A	C	M	U	U
Item description	A	U	M	U	U	C	U	U
Item quantity	U	U	M	A	U	U	C	U
Item price	U	U	M	A	U	U	C	U
Vendor								
Vendor address	U	U	M	M	U		C	
Vendor code	U	U	M	A	C	U	U	U
Vendor name	U	U	M	A	U	U	C	U

Roles
(**C**)reate/modify, (**A**)pprove, (**U**)se, (**M**)onitor

Captures Data
Triggers Resolution and Update
Maintains Quality

Using Software Integrating Process, Control, and System Documentation

The compliance manager (an assigned duty of the CFO, not a full-time role) of a services provider with annual revenues of $50 million uses a documentation software tool that promotes clear understanding and assessment of processes and efficiency of documentation. The software facilitates an integrated depiction of a process, related controls, and system documentation, identifying inputs to the process, processing activities, controls, and supporting information systems.

Captures Data
Triggers Resolution and Update
Maintains Quality

Risk Assessment Considers Changes in Information Systems

The CEO of a specialty resin company with operations in nine countries continually reviews risks to the company. In each monthly lead staff meeting, the CEO asks senior managers to comment on their identification of new risks, including those related to changes in systems, personnel processes or activities. The CEO discusses his insights on risks facing the company, including those that impact on financial reporting, and together any needed risk responses are developed.

Principle 17
Internal Communication

Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.

Attributes of the Principle

Communicates with Personnel – Management communicates to all personnel, particularly those in roles affecting financial reporting, that internal control over financial reporting must be taken seriously.

Communicates with Board – Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to financial reporting objectives.

Includes Separate Communication Lines – Separate communication channels are in place and serve as a "fail-safe" mechanism in case normal channels are inoperative or ineffective.

Accesses Information – The board has access to information sources outside of management, on a regular basis and as needed, including access to the external auditors, the internal auditors, and other relevant parties (such as regulatory authorities).

Approaches to Applying the Principle

Communicating Information Regarding Financial Reporting Objectives

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Management communicates information about the company's financial reporting objectives, relevant internal control policies and procedures and how they work, and related individual responsibilities. Such mechanisms include:

- Broadcast e-mails and/or voice mails from management reinforcing the company's commitment to internal control over financial reporting, including updates on both internal and external matters.
- Regular organization-wide conference calls or webcasts addressing similar matters.

Communicating Through an Intranet Site

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Management develops and maintains an intranet site, accessible to all appropriate personnel, for disseminating information regarding the company's internal control processes over financial reporting. Management reviews and confirms that the code of conduct and related content dealing with integrity and ethical values is clearly stated on the site.

Reviewing Financial Information with the Audit Committee

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

At regular audit committee meetings, the CFO reviews financial information, analysis and related internal control, and enters into open discussion on all matters of directors' interest.

Communicating Between the Board and Internal Auditor

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

The board of directors and the chief internal auditors meet periodically and whenever events or circumstances warrant. These meetings are used to discuss, in an open environment, the internal auditors' observations about the company's internal control over financial reporting.

Communicating the Whistle-blower Program to Company Personnel

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

The company maintains a "whistle-blower" process that enables employees to communicate misconduct, including matters relating to reliable financial reporting. To enhance employee awareness, a description of the hotline's purpose and its phone number are included in the employee handbook, on the company's intranet, and/or on signs posted in high-traffic areas throughout the premises. The hotline is managed internally or by a third party.

Communicating Alternative Reporting Channels

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Management provides an alternative to reporting to a line manager – either a coaching or mentoring program or a professional or technical reporting channel – so that employees are confident that they will be heard.

Developing Guidelines for Communication to the Board

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

The board of directors develops guidelines for materials it expects to receive. Management submits briefing materials at least 10 days in advance to allow directors sufficient time to review and formulate questions. In addition, management provides a summary for any briefing material that exceeds three pages in length.

Consulting with Outside Advisors

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

The audit committee consults with outside advisors whenever committee members feel management might lack the capability to adequately address an important issue or when an area of GAAP is not clearly defined.

Examples of Applying the Principle

Using Communications Programs to Reinforce Internal Control

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

The CEO of a healthcare services provider communicates through newsletter and personal visits to staff locations and training program sites. The CEO uses these venues to reinforce the meaning of internal control over financial reporting, how it relates to laws and regulations, and what is expected of the organization and of all employees.

Using a Finance Conference to Discuss and Reinforce Internal Control

A 300 person broadband infrastructure company holds a semiannual meeting led by the CFO and controller. Business unit finance staff attend the meetings, which the CFO uses as a forum to provide an update on the business. Topics discussed include:

- Key objectives for the next six months
- Reinforcement of the company's policies related to ethics and integrity
- Importance of internal controls
- Changes to the internal control structure

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Facilitating Communication Between the CEO and Board

The CEO and board chair of a $130 million manufacturer of medium- and high-speed printing solutions talk at least monthly and more frequently if the need arises. Board members raise questions in advance which the chair organizes and presents to the CEO, who in turn directs them to members of the management team. The managers respond directly, copying the CEO and identifying any needed follow-up actions to be taken. Directors obtain the needed information, and key managers gain more exposure to the board.

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Establishing a Mentoring Program to Facilitate Upstream Communication

A $200 million designer and distributor of sports apparel established a mentoring program where each employee is assigned a coach; they meet periodically or as needed to discuss specific topics such as the employee's performance and goals. All staff involved in the financial reporting process are assigned a mentor with financial reporting and internal control experience. The program provides an alternative to the employee's line supervisor for discussing and reporting concerns on matters such as compensation, operations, or controls.

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Using a Staff Council to Facilitate Upstream Communication

A manufacturer of steel products for the transportation, construction, and utility markets holds quarterly town hall meetings where the CEO and other members of senior management meet with staff to discuss "hot topics" affecting the company. Senior management uses these meetings to emphasize its commitment to ethics and integrity, provide a brief business update, and solicit feedback on policy changes being considered. Staff may voice questions or concerns received from personnel in their spheres of responsibility, provide suggestions to improve processes, and provide feedback. Management is then better able to evaluate how staff observations are impacting internal control over financial reporting. Meeting minutes are published in the company's newsletter distributed to all employees monthly.

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Accessing Third Parties for Assistance

A mining company with several development projects but only one operating mine periodically enters into joint ventures, some of which are potential variable interest entities. Management has chosen not to hire a full-time staff member or train existing staff to determine the appropriate accounting for such entities, and instead engaged an expert to advise management on the proper accounting for these equity investments. The company's management considers the third party's advice, assesses recommendations made, and makes informed decisions on implementation. The recommendations and management's actions are provided to the audit committee for review.

Communicates with Personnel
Communicates with Board
Includes Separate Communication Lines
Accesses Information

Principle 18
External Communication

Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Attributes of the Principle

Provides Input – Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts and others, providing management and the board with important information on the effectiveness of internal control over financial reporting.

Independently Assesses – Where internal control over financial reporting is assessed by external auditors, information relevant to the assessment is communicated to management and the board.

Approaches to Applying the Principle

Communicating the Whistle-blower Program to Outside Parties

Provides Input
Independently Assesses

Management makes a whistle-blower phone number or e-mail address available to customers, suppliers, and other external parties to facilitate feedback. The contact information is disseminated via the company's website and invoices sent to customers. This enables receipt of important information from parties doing business with the company, such as vendors who feel they have not been treated fairly, receive pressure for kickbacks, are subject to other improprieties, or are aware of improper financial reporting.

Surveying Outside Parties

Provides Input
Independently Assesses

Management surveys customers, vendors and others on their perception of the integrity and ethical values company personnel. This survey process is controlled by company personnel independent of the main customer/vendor contacts.

Reviewing External Audit Communications

Provides Input
Independently Assesses

Following the external auditor's review of management's certification process and independent evaluation of internal control effectiveness, management receives a memorandum on significant matters identified during the course of the work. The matters are discussed at a subsequent audit committee meeting, where management and external auditor personnel address the findings and proposed resolutions.

Examples of Applying the Principle

Facilitating Communication with Customers

A manufacturer and marketer of strength and cardiovascular fitness equipment has a policy where at least two members of management independent of the customer's primary contact communicate with each customer as necessary, but at least annually. These discussions not only provide a sounding board for the company's customers, but also enable the company to update its understanding of the customer's business and external factors affecting the customer. This has led to sharing of information to improve the accuracy and timeliness of sales and receivables information, and also has served to strengthen customer relationships. These discussions are evidenced through a memo on each conversation, including customer contact, date, and topics discussed, including any action items from either party and their resolution.

Provides Input
Independently Assesses

Facilitating Communication with External Parties

A manufacturer and retailer of branded and private label vitamins and nutritional supplements includes on its website a telephone number that can be called with questions, concerns, complaints, and the like. Matters reported are recorded and addressed. A log of entries and report of significant issues related to illegal acts or financial reporting improprieties is provided to the audit committee for review and discussion.

Provides Input
Independently Assesses

Communicating with Regulators

As a result of a regulator's examination, a registered investment adviser was informed that the firm was not in compliance with rules requiring documentation of certain compliance policies and procedures, with the regulator holding that the firm's compliance procedures were too generic. After conferring with outside counsel, the CFO discussed the matter with the regulator, and reached agreement on the firm's plan and timeline to develop an appropriate compliance policies and procedures manual.

Provides Input
Independently Assesses

V. Monitoring

Internal control systems are monitored to assess the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

Ongoing monitoring occurs in the normal course of recurring management activities. Managers of many smaller businesses have high-level first-hand knowledge of company activities, and their close involvement in operations positions them to identify variances from expectations and potential inaccuracies in reported financial information.

Some smaller companies have an internal audit function which as part of its regular duties performs procedures that help determine the functioning of the other internal control components. Where no internal audit function exists, managers responsible for a business unit or function might perform an evaluation of the effectiveness of certain controls within their sphere of responsibility.

Where a company assesses its internal control over financial reporting pursuant to Sarbanes-Oxley Section 404, elements of the monitoring component, particularly any separate evaluations that might be performed, may be useful in determining how to design and plan the assessment process.

Two principles relate to the monitoring component:

19. **Ongoing and Separate Evaluations** – Ongoing and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time.

20. **Reporting Deficiencies** – Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

Guidance useful in implementing or assessing the application of the principles is provided in the balance of this chapter, with additional illustrative guidance included in Volume III.

Principle 19
Ongoing and Separate Evaluations

Ongoing and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time.

Attributes of the Principle

Integrates with Operations – Ongoing monitoring is built into the company's operating activities.

Provides Objective Assessments – Evaluations provide an objective consideration of internal control over financial reporting.

Uses Knowledgeable Personnel – Evaluators understand the components being evaluated and how they relate to activities supporting the reliability of financial reporting.

Considers Feedback – Management receives feedback on the effectiveness of internal control over financial reporting.

Adjusts Scope and Frequency – Management varies the scope and frequency of separate evaluations depending on the significance of risks being controlled, the importance of the controls in mitigating those risks, and the effectiveness of ongoing monitoring.

Approaches to Applying the Principle

Using Metrics to Track performance

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Management establishes supervisory activities, consisting of recording metrics about control in processes so that current performance can be tracked and compared with target performance.

Developing and Implementing Control Charts

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Management develops and implements control charts for reviewers – usually supervisors of those with first-level accountability for processes and activities and their controls – to use in considering whether control performance is on track, the right metrics are being monitored, and deviations are being investigated and resolved.

Relating Metrics to Financial Reporting

Management confirms that operations metrics that are monitored have reasonable correlation to financial reports and thus can be used as an indicator of potential deficiencies in financial reporting.

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Using Self-Assessments

Management develops a self-assessment questionnaire for a business process for use by personnel involved in executing controls.

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Using Computer Network Testing

Management periodically tests its computer network by performing a penetration review to identify weaknesses in internal controls regarding external connectivity. Identified security issues concerning access to financial data are addressed and resolved in a timely manner.

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Using Internal Audit

Management uses an internal audit function to provide an objective perspective on key elements of the internal control system. Internal audit reports are distributed to senior management and the audit committee.

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Determining Scope and Frequency of Separate Evaluations

Management groups financial statement accounts as higher, moderate, and lower risk. Management considers past effectiveness of control activities in managing risks and the extent of ongoing monitoring within the associated processes. From this, management sets a schedule for conducting separate evaluations of specific processes and control activities, with higher risk processes reviewed by the internal audit function.

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Examples of Applying the Principle

Identifying Key Indicators to Improve Performance Monitoring

The CFO of an integrated marketing services company identified five key performance/control indicators – dealing with management of receivables, expenses, pricing, engagement staffing, and staff productivity – having high correlation with financial reporting outcomes. Their use has led to improved controls and substantive improvement in business performance.

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Using Built-in Operating Measures and Key Control Indicators

The CFO of a manufacturer of food products with annual revenues of $75 million uses operating measures and key control indicators (KCIs) for major accounting and financial processes, including those processing accounts receivable, payroll, and accounts payable, and financial statement preparation. Accounts payable KCIs, for example, focus on the accuracy, timeliness, completeness, and compliance of documents received for vouching and checks prepared, with performance tracked to targets. Results are shared with the management team and used for performance appraisals and related development programs.

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

Ongoing Monitoring as an Indicator of Control Effectiveness

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

A dairy processor performs inventory cycle counting daily. These counts confirm that packaging supplies are available for short-term production plans, and that supplies and ingredient usage agrees with production reports. The count team follows a systematic process to check higher-volume and currently used items both more frequently and consistently with the timing of expected use. These cycle counts also support the full, quarterly inventory count. All counts are performed "blind" where the count team does not have access to the perpetual inventory system balances. When a cycle count is completed, the inventory manager compares the results to the quantities in the perpetual inventory system, investigates differences, and makes any needed adjusting entries. The cost accountant and controller consider any weaknesses in the operation of inventory controls, and recommend corrective actions.

Using Operating Information in Monitoring

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

A manufacturer and importer of agricultural equipment's controller's function maintains a sales target report. Weekly, the controller reconciles actual sales reported by the accounting system with the targets, with significant variances investigated with assistance of regional sales managers.

Using Matrices to Relate Operating Information

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

A $75 million manufacturer of industrial machinery parts uses a set of operating matrices by business process, with each matrix containing a series of tasks assigned to the appropriate managers for action. The matrix for the production inventory process, for example, includes costs associated with tooling, where the warehouse manager monitors usage of tools during production -- how often they are needed, who requested them, and from where they are being purchased – and considers this information when reviewing tooling costs included in inventory. During monthly meetings the matrices are reviewed, with the task owners, CFO and President discussing recent progress and expected changes over the coming month. The CFO makes decisions on tasks to be added or removed from the matrices.

Using Firsthand Knowledge of a Business

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

A manufacturer of alternative fuel products and systems to the transportation market has 720 employees between union labor, supervisors, managers, and executives. All plants run two shifts six days a week, with each having approximately the same number of employees. The CFO has been with the company for ten years and thoroughly understands its business processes, including the payroll process, and reviews weekly payroll summary reports prepared by the centralized accounting function. With the company's flat organizational design and smaller size; the CFO's background with the company and his understanding of the seasons, cycles, and workflows; and close familiarity with the budget and reporting processes, the CFO quickly identifies any sign of improprieties with payroll and their underlying cause – whether related to a particular project, overtime, hiring, layoffs, and so forth. The CFO investigates as needed to determine whether errors or irregularities have occurred and whether any internal control has not operated effectively, and takes corrective action.

Determining Scope and Frequency of Separate Evaluations

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

From time to time the board of a designer, manufacturer, and distributor of precision components and assemblies for use in aerospace applications directs the company's internal audit function to perform separate evaluations of specified high risk business processes. The scope and frequency depend primarily on the significance of the related risks and importance of the controls in reducing risks to an acceptable level. The internal audit director determines whether the internal audit or other staff selected have sufficient objectivity with regard to the business processes to be reviewed, and have adequate understanding of the process, the overall internal control structure, and the objectives of the review.

Upon completion, the internal audit director provides a report on the process controls to senior management and the board covering:

- Scope of the work, including identification of the controls evaluated.
- Descriptions of major risks and appropriateness of the controls.
- Identified deficiencies and management's response and proposed remediation.

Cross-Business-Unit Reviews

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

A $120 million manufacturer and distributor of animal feed products uses personnel from different business units to evaluate internal control over financial reporting. Accounting personnel from business unit A, for example, periodically evaluate internal controls of business unit B. Reviews are performed in accordance with the International Standards for the Professional Practice of Internal Auditing established by The Institute of Internal Auditors. The review teams report findings and recommendations to management and the audit committee.

Outsourcing Internal Audit

Integrates with Operations
Provides Objective Assessments
Uses Knowledgeable Personnel
Considers Feedback
Adjusts Scope and Frequency

A $180 million operator of laundry facilities outsources its internal audit activity. To monitor and control the outsourced function, the CEO and audit committee chair meet quarterly with the outsourcer's engagement leader. The discussion covers work performed, findings, additional work planed or suggested, and any risks or concerns the engagement leader may have along with related recommendations.

Principle 20
Reporting Deficiencies

Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

Attributes of the Principle

Reports Findings – Findings of internal control deficiencies are reported both to the individual who owns the process and related controls and is in position to take corrective actions, and to at least one level of management above the process owner.

Reports Deficiencies – Significant deficiencies are communicated to top management and the board or audit committee.

Corrects on a Timely Basis – Deficiencies reported from both internal and external sources are considered and timely corrective actions taken.

Approaches to Applying the Principle

Reporting Information from Alternative Channels

Reports Findings
Reports Deficiencies
Corrects on a Timely Basis

Management establishes an alternative channel for reporting deficiencies sensitive in nature, such as illegal or improper acts. Such reports are directed to a member of senior management or the board, depending on the nature of the matter and persons involved.

Reporting Deficiencies to Various Levels in the Company

Reports Findings
Reports Deficiencies
Corrects on a Timely Basis

Management establishes a practice where all financial reporting deficiencies regardless of materiality are reported to the responsible manager and at least one level of management above, both of whom are positioned to take corrective action. The nature of the matter and materiality dictate the levels to which the deficiency is reported.

Developing Guidelines for Reporting Deficiencies

Reports Findings
Reports Deficiencies
Corrects on a Timely Basis

Management develops a list of control deficiencies that seriously threaten the reliability of financial reporting, which if they occur are required to be reported to senior management and the board. Types of deficiencies fitting this criterion include deficiencies relating to illegal or otherwise improper acts, significant loss of assets, and improper external financial reporting.

Examples of Applying the Principle

Reporting Control Deficiencies to Management

A consumer electronics retailer with 23 stores organized teams with employees having different functional responsibilities, with the team leader being a member of management. The teams devote approximately 30 minutes per month to discuss, among other things, ways to address control deficiencies and improve the internal control structure. Team leaders report deficiencies and recommendations to the appropriate managers, based on the nature and materiality of the matters.

Reports Findings
Reports Deficiencies
Corrects on a Timely Basis

Reporting Control Deficiencies and Resolution to the Board

The board of a 570 employee manufacturer and distributor of specialty tools for the home improvement market oversees management's tracking of control deficiencies, periodically receiving a log of the deficiencies and resolution. The board reviews the log, including information on notification of the responsible party and his/her supervisor, and corrective action to be taken, as well as status of prior periods actions.

Reports Findings
Reports Deficiencies
Corrects on a Timely Basis

Reporting Deficiencies to the Board

A provider of air transportation services' management periodically develops a report of significant deficiencies and material weakness, along with a summarization of minor deficiencies, and presents it to the board for review.

Reports Findings
Reports Deficiencies
Corrects on a Timely Basis

Appendices

A. Methodology
B. Consideration of Comment Letter
C. Glossary of Selected Terms
D. Acknowledgments

Appendix A
Methodology

Background

Soon after companies began to consider how best to comply with the internal control reporting requirements of the Sarbanes-Oxley Act, it became readily apparent that smaller public companies faced unique challenges. The SEC Chief Accountant, having considered the surrounding issues, suggested that COSO initiate a project to develop guidance designed to help smaller companies use COSO's Internal Control – Integrated *Framework* in connection with complying with Sarbanes-Oxley Section 404 requirements. COSO agreed, and in January 2005 engaged PricewaterhouseCoopers to conduct the project and write this report.

This report is designed to help management of smaller companies deal with unique challenges in maintaining effective and efficient internal control over financial reporting. This guidance does not replace or modify the *Framework*, but rather assists management in understanding how to cost-effectively use the *Framework* to achieve their financial reporting objectives.

Project Structure

Throughout the project significant input was obtained from executives of many smaller organizations, including chief executive officers, chief financial officers, controllers, and internal auditors. Input also was received from investors, legislators, regulators, lawyers, external auditors, consultants, and academicians. Also throughout the project, the PricewaterhouseCoopers project team received advice and counsel from an Advisory Task Force reporting to the COSO Board, and from the COSO Board. The Task Force consisted of sixteen members with experience in small business.

Supplementing the four-phase project plan described below:

- A forum was held with invitees from a wide range of small businesses to enable the project team, as well as the Task Force and COSO Board to better understand the unique challenges smaller businesses face in developing, implementing and assessing internal control over financial reporting.
- A number of Task Force members and COSO Board members attended an SEC roundtable on internal control reporting requirements that solicited input on application of Sarbanes-Oxley Section 404.
- Drafts of the guidance were reviewed by managers of and individuals working with smaller businesses.
- Preliminary versions of the guidance were reviewed with a number of organizations, including the AICPA's major firm group of fifty larger public accounting firms specializing in working with smaller businesses.

At all key project milestones, the project team communicated with and received feedback from the Task Force and COSO Board.

Approach

The project consisted of four phases:

Research – This phase identified, through literature reviews and public forums, challenges facing smaller businesses in using the *Framework*. In this phase the project team analyzed information, contrasted approaches, and identified critical issues and concerns.

Building and Designing – The project team developed the guidance, including principles, attributes, approaches, and examples related to effective and efficient internal control over financial reporting. The guidance was reviewed with key user and stakeholder groups, and reactions and suggestions for enhancement were obtained.

Preparation for Public Exposure – The project team reviewed the draft guidance with several companies, and used the feedback to refine the document.

Finalization – This phase encompassed issuing the guidance for public exposure for a 60-day comment period. The project team reviewed and analyzed the comments and identified needed modifications. The project team then revised the document for the COSO Task Force's and COSO Board's final review and acceptance.

As expected, many different and sometimes contradictory opinions were expressed on fundamental issues – within a project phase and between phases. The project team, with Task Force and COSO Board oversight, carefully considered the merits of the positions put forth, both individually and in the context of related issues, embracing those that facilitated development of a relevant, logical, and internally consistent document.

Appendix B
Consideration of Comment Letters

A draft of this document was exposed for public comment from October 26, 2005 through January 15, 2006. The 176 responses received contain hundreds of individual comments on a wide variety of matters. Each comment was considered in formulating revisions to the final guidance. This appendix summarizes the more significant issues and resulting modifications reflected in this final report and provides perspective on why certain views were accepted over others.

Principles, Attributes, Approaches and Examples

For each of the *Framework*'s five components, the exposure draft provided four sections: principles; attributes; approaches; and examples. Respondents were generally supportive of this organization, although some called for expanded description of the principles and direction as to whether particular principles are unique to smaller businesses. Other respondents stated they believed that there was some redundancy across principles. And still other respondents expressed concern that the approaches and examples would be viewed as requirements for effective internal control over financial reporting in smaller businesses.

The final document retains the exposure draft's organization, and does not elaborate further on the fundamental principles. The principles are derived from the *Framework*, which includes descriptive material, and are supported by the attributes, approaches and examples, which together are deemed sufficient to enable readers to understand the substance of the principles.

Regarding whether the principles are unique to smaller businesses, it is determined that they are not. Rather, because they reflect key concepts established in the *Framework*, principles are applicable to companies of every size, including smaller businesses. Thus, the guidance does not reflect the view that smaller organizations have a unique set of guiding principles for internal control.

As for redundancy, it is agreed some overlap existed among certain of the principles, and opportunities to combine principles within components were identified: Three principles in the Information and Communication section were merged, two in the monitoring section were merged, and three under roles and responsibilities were incorporated into others. Accordingly, the final document contains twenty principles, reduced from the exposure draft's twenty-six.

Regarding the potential that approaches and examples might be viewed as being "required," verbiage has been added to further emphasize that the guidance inherent in the approaches and examples is merely illustrative of how management of a smaller business might decide to view effective internal control.

Assessing Effectiveness of Internal Control over Financial Reporting

Some respondents expressed views regarding what constitutes effective internal control over financial reporting different from that set forth in the exposure draft. In that regard, some suggested that in smaller companies not all principles or attributes need be present for effective internal control, with some of those respondents expressing the view that because certain principles are more important than others, the "less important" principles need not be present. Other respondents suggested that an assessment of effectiveness is dependent on following a top-down process as advocated by the SEC and PCAOB.

The criterion for effectiveness – being the presence and effective functioning of each of the five components to the extent that management has reasonable assurance that financial statements are being prepared reliably – is established in the *Framework*, and that document remains the definitive reference for determining effectiveness of internal control. Because the twenty principles contained in this guidance are drawn directly from the *Framework*'s components, all principles are relevant to effective internal control, regardless of company size, and the final guidance carries forward this concept. It is recognized, however, that not every principle applies equally to every company. The final guidance states that management needs to evaluate the company's internal control system in relation to the *Framework*, and that focusing on the twenty principles is useful in making that evaluation. The final guidance does not state that a company lacking a particular principle necessarily does not have effective internal control. Rather, it says that when a principle is not achieved, an internal control deficiency exists, and such deficiencies should be evaluated to determine whether they rise to the level of significant deficiency or material weakness.

The principles, together with the related attributes, approaches and examples, are designed to help managements of smaller businesses more readily recognize what is needed for effective internal control – and how to achieve that goal more efficiently. It is expected that this guidance will be useful to management in following a risk-based approach in assessing internal control effectiveness, as suggested by the SEC and PCAOB, rather than viewing such an approach as a new standard for what constitutes internal control effectiveness.

Cost Effectiveness of Approaches and Examples

Some respondents commented that the examples in the exposure draft did not consistently portray ways to reduce cost, and that the guidance needs to clarify what users can expect in terms of cost savings.

The examples in the exposure draft were intended to describe cost-effective ways to achieve effective internal control over financial reporting. It is recognized that for every company, including smaller ones, effective internal control comes with a cost, and the guidance is designed to enable management of smaller companies to manage the incremental costs. Certainly, use of some approaches and examples will be more cost-effective for some companies than others, and management may decide whether to apply one or more of the approaches and use selected examples presented in this guidance or to develop its own ways of applying the principles.

The final guidance emphasizes that small businesses can implement cost-effective internal control, that effective internal control over financial reporting offers significant benefits, and

that management should consider costs and benefits together without focusing exclusively on cost. The narrative in the guidance has been enhanced to better describe means by which smaller companies can more efficiently achieve effective internal control, and the approaches and examples have been sharpened to better illustrate how that can be done.

Entity-Wide Controls and Management Oversight

Some respondents commented that there is a need for additional emphasis on how entity-wide controls and the role of management oversight adequately take the place of other controls. Other respondents expressed an opposing view, stating that there was too much emphasis on the relevance of entity-wide controls and management oversight, presenting a risk of over reliance.

The final guidance contains added discussion on how management gains comfort from multiple points of reliance, including entity-wide controls, and retains the considerable coverage of the use of entity-wide controls in Volume II's Control Environment and Monitoring chapters and in Volume III.

Monitoring

Some respondents said the level of discussion on monitoring was too limited and called for additional guidance, especially for monitoring at the entity-level. Respondents' comments suggested that some confusion remains in distinguishing monitoring of internal control and monitoring company performance.

It was concluded that the exposure draft's Monitoring chapter appropriately dealt with monitoring internal control (rather than monitoring company performance). Additional discussion, however, was added to clarify what monitoring is and means by which management can efficiently monitor other components of a company's internal control system. And, as noted earlier, in an effort to reduce the number of principles, two principles in the monitoring chapter were combined.

Retaining a Management Focus

Some respondents commented that a greater management-centric focus is needed, with less emphasis on the role the auditor. Others respondents were seeking greater alignment with an auditor's perspective, in general and with respect to AS No. 2 in particular.

The final document reflects a clearer direction to management's actions to develop and implement an effective internal control system or evaluate its effectiveness. While the guidance might be useful to auditors, it is not directed to them, nor is it intended to interpret AS No. 2. The final document is designed to better make this distinction.

Some respondents suggested that additional guidance should be provided as to what constitutes sufficient documentation. It was decided that discussion on documentation should not be expanded for several reasons. First, the *Framework* provides little discussion on appropriate levels of internal control documentation; second, the nature and extent of documentation appropriately varies extensively depending on a company's circumstances; and third, the type of documentation expected to be examined by auditors in auditing internal control systems is addressed in AS No. 2.

Segregation of Duties

Some respondents called for added discussion on ways to compensate for controls not in place, especially those relating to segregation of duties.

Because of the importance of this topic, the challenges surrounding segregation of duties are more fully recognized and the discussion and examples of related controls more fully developed in the final document.

Information Technology

Some respondents commented that information technology is an area of significant concern for many smaller companies, and additional guidance is needed.

The final document contains added guidance on information technology, including discussion on differences between less and more complex information technology environments. This discussion complements the already significant focus on IT controls in the document, including many of the examples in Volume II. Because the section on information technology already was long in relation to others, in order to provide better balance, discussion of application and general computer controls and certain of the examples previously in Volume II are now included in Volume III. That volume includes additional tools for evaluating information technology controls in both a less complex and more complex information technology environment.

Document Length

Some respondents expressed concern on the overall length of the document, stating that managers of smaller businesses might find the material too voluminous. Many respondents suggested breaking the document into several volumes rather than removing text.

It was decided not to cut back on document length, but rather to make it more user friendly. Sections aimed at more senior personnel have been streamlined and material for other managers better organized to be more useful as a reference document. The final document consists of three volumes. Volume I contains the Executive Summary geared to members of boards of directors and senior management seeking a high level summary. Volume II contains guidance directed at managers closely involved in developing or assessing their company's internal control systems. The first chapter of Volume II contains textual guidance on cost-effective internal control, followed by a chapter on each internal control component listing relevant principles of internal control together with attributes of the principles, approaches that can be used to achieve the principles and supported by illustrative examples. Volume III contains detailed illustrative evaluation tools and templates. The material in the component chapters of Volume II and in Volume III is directed for use as a reference tool to be used when considering controls in particular areas.

Appendix C
Glossary of Selected Terms

The *Framework* includes in an appendix a glossary of selected terms. In addition to the terms used and defined in the *Framework*, the following terms are used in this guidance, defined as follows:

Attributes – characteristics associated with and supporting a principle.

Compensating Controls – Compensating controls are considered in the course of evaluating the overall risk to reliable financial reporting. These are controls that serve to accomplish the objective of another control that did not function properly, helping to reduce risk to an acceptable level.

Entity-wide Controls – Controls that occur at the entity level of a company and have a pervasive influence across the organization. Entity-wide controls may exist in any of the five components of internal control.

Internal Control over Financial Reporting – A process, effected by a company's board of directors, management and other personnel, designed to provide reasonable assurance regarding the reliability of published financial statements.

Process Level Controls – Controls within an organization's process, operating at a lower and more targeted level than entity-wide controls.

Principles – Fundamental concepts associated with effective internal control over financial reporting and drawn directly from the five components of the *Framework*.

Risk – The possibility that an event will occur and adversely affect the achievement of (financial reporting) objectives.

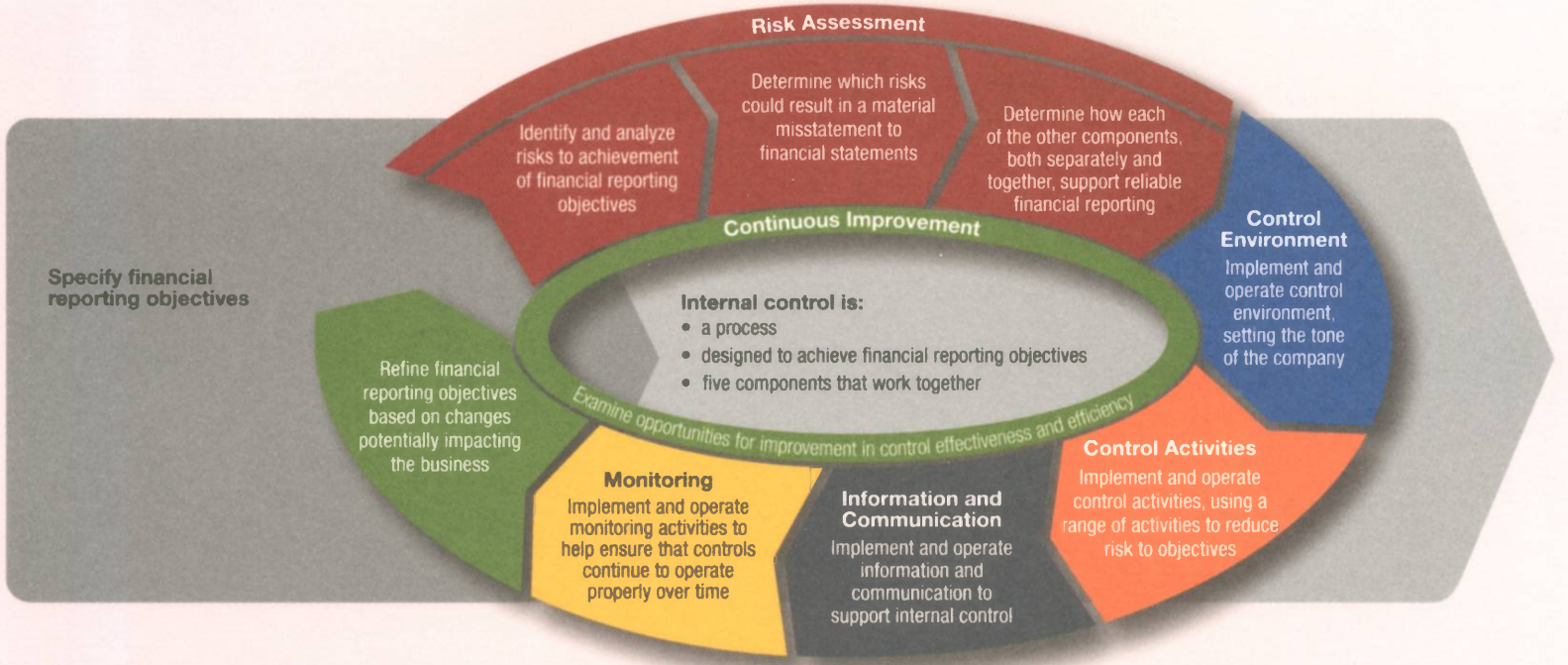
Statement on Auditing Standard (SAS) 70 Report – A report, prepared by an independent auditor in accordance with the American Institute of Certified Public Accountants SAS No. 70, on specified internal controls of a service organization.

Stock Exchange – US-based stock exchanges such as American Stock Exchange (AMEX), New York Stock Exchange (NYSE), or NASDAQ.

Appendix D
Acknowledgments

The COSO Board, Task Force, and PricewaterhouseCoopers LLP gratefully acknowledge the many executives, legislators, regulators, auditors, academics, and others who gave their time and energy to participating in and contributing to various aspects of the study. Also recognized are the considerable efforts of the COSO organizations and their members who participated in workshops and meetings, and provided comments and feedback throughout the development of this guidance. Special acknowledgement goes to Dennis L. Neider for his early contributions as a representative of the Institute of Management Accountants.

Many other PricewaterhouseCoopers partners and staff provided important input to this framework, including Lisa Beauregard, Myra Cleary, Carlo di Florio, Robert Fish, and Jonny Frank. We also acknowledge the contribution of Richard M. Steinberg, Founder and Principal of Steinberg Goverance Advisors Inc. and former PricewaterhouseCoopers partner.



Risk Assessment

8. **Identify financial reporting objectives**
   Complies with GAAP, supports information disclosures, reflects company activities, is supported by relevant financial statement assertions and considers materiality 44
9. **Identify and analyze financial reporting risks**
   Includes business processes, personnel and information technology, involves appropriate levels of management, considers both internal and external factors, estimates likelihood and impact, and triggers reassessment . . . 47
10. **Identify and assess the risk of fraud as it affects the company**
    Considers incentives and pressures, risk factors, and establishes responsibilities and accountability 52

Control Environment

1. **Integrity and ethical values are developed and understood**
   Articulates values, monitors adherance, addresses deviations 20
2. **Board of directors understand and exercise oversight**
   Defines authorities, operates independently, monitors risk, retains financial reporting expertise, oversees quality and reliability and oversees audit activities 23
3. **Management philosophy and operating style support internal control**
   Sets the tone, influences attitudes towards accounting principles and estimates and articulates objectives 29
4. **Organizational structure supports internal control**
   Establishes lines of financial reporting and establishes structure 31
5. **Financial reporting competencies are retained**
   Identifies competencies, retains individuals and evaluates competencies 33
6. **Authority and responsibility are assigned**
   Defines responsibilities and limits authority 35
7. **Human resource policies and practices facilitate internal control**
   Establishes human resource practices, recruits and retains, adequately trains, and evaluates performance and compensates 38

Control Activities

11. **Control activities integrate with risk assessment**
    Mitigates risks, considers all significant points of entry into the company's G/L and information technology 56
12. **Control activities are selected and developed**
    Considers range of activities, includes preventive and detective controls, segregates duties, and considers cost vs. benefit 58
13. **Policies are established and communicated and result in management directives being carried out**
    Integrates into business processes, establishes responsibility and authority, occurs on a timely basis, thoughtfully implements, investigates exceptions, and periodically reassesses 62
14. **Information technology controls are designed and implemented**
    Includes application controls, considers general computer operations, and includes end-user computing 66

Information and Communication

15. **Financial reporting information is identified, captured, used and distributed**
    Captures data, includes financial information, uses internal and external sources, includes operating information, and maintains quality 76
16. **Internal control information is identified, captured, used and distributed**
    Captures data, triggers resolution and update, and maintains quality 78
17. **Internal communication supports execution of internal control**
    Communicates with personnel and board, includes separate communication lines, and accesses information 81
18. **Matters affecting achievement objectives are communicated**
    Provides input and independently assesses 84

Monitoring

19. **Ongoing and/or separate evaluations enable management to determine function of internal control**
    Integrates with operations, provides objective assessment, uses knowledgeable personnel, considers feedback and adjusts scope and frequency 88
20. **Internal control deficiencies are identified and communicated**
    Reports findings and deficiencies, and corrects on a timely basis 92

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

www.coso.org

990017